

Stenholm Valtteri


ETELÄ-KYMENLAAKSON  
AMMATTIOPISTON LVI-  
AUTOMAATION ETÄVALVONTA-  
MAHDOLLISUUKSIEN KARTOITUS

Opinnäytetyö  
Talotekniikan koulutusohjelma


Toukokuu 2016



# KUVAILULEHTI

 <b>MAMK</b> University of Applied Sciences	<b>Opinnäytetyön päivämäärä</b>  20.5.2016
<b>Tekijä(t)</b> Valtteri Stenholm	<b>Koulutusohjelma ja suuntautuminen</b> Talotekniikka
<b>Nimeke</b>  Etelä-Kymenlaakson ammattiopiston etävalvontamahdollisuuksien kartoitus	
<b>Tiivistelmä</b> <p>Rakennusautomaationjärjestelmien etähallinta mahdollistaa rakennuksen toimintojen tarkastelemisen sekä niiden muuttamisen ajasta taikka paikasta riippumatta. Tämän opinnäytetyön tavoitteena oli kartoittaa eri tapoja toteuttaa Etelä-Kymenlaakson ammattiopiston kampusten LVI-automaation etähallinta.</p> <p>Rajauksista huolimatta työn laajuus eri laitteistoista sekä ohjelmistoista johtuen oli jo alusta alkaen huomattavan suuri. Tästä johtuen opinnäytetyössä pyrittiin pitäytymään pääosin yleisellä tasolla huomioimalla kuitenkin Ekamin kampusten automaatiojärjestelmien erityispiirteet. Opinnäytetyötä varten tehtiin kattava kirjallisuuskatsaus kohderakennusten automaatiojärjestelmien protokollista sekä yleisistä tietoliikennestandeista. Työtä varten haastateltiin kampusten automaatiojärjestelmäratkaisuihin vastaavia alan asiantuntijoita, joiden kanssa selvitettiin useita vaihtoehtoja toteuttaa toimiva ratkaisu internetin yli tapahtuvaan LVI-automaation hallintaan. Tämän lisäksi suoritettiin Ekamin LVI-automaatiolaitteiden kartoitus. Tämän perusteella voitiin luoda hyödyllinen topologiakartta, josta on nopeasti nähtävissä nykyisten järjestelmien keskeisimmät osat.</p> <p>Insinööritöiden edetessä kävi selväksi, että mahdollisia etähallintaan tarkoitettuja tuotteita on markkinoilla runsaasti. Monet näistä mahdollistivat usean eri järjestelmän yhdistämisen toisiinsa, jolloin toisistaan eroavia toteutusvaihtoehtoja oli monia. Työhön pyrittiin saamaan käytettävissä olevien resurssien puitteissa mahdollisimman monipuolinen otanta laite- ja ohjelmistopohjaisista ratkaisuista yhden sekä useamman laitteen ohjaamiseen.</p> <p>Työlle asetetut tavoitteet saavutettiin ja kolme toteutuskelpoista etähallintavaihtoehtoa valittiin lähempää tarkastelua varten. Näistä helpoin olisi ohjelmistopohjainen TeamViewer, joka mahdollistaisi LVI-laitteiden hallinnan valvomotietokoneiden kautta. Kattavampia vaihtoehtoja edustavat kahden eri valmistajan keskitetyt LVI-automaatioratkaisut. Mikäli järjestelmän kokonaisvaltaiseen uudistamiseen päädytään, tulisi tilaajan tehdä yhdessä alan asiantuntijoiden kanssa yksityiskohtainen vaatimusten määrittely, ennen hankkeen toteuttamista.</p>	
<b>Asiasanat (avainsanat)</b>  LVI-automaatio, etähallinta, etäyhteys, BACnet, Modbus	
<b>Sivumäärä</b>  44+2	<b>Kieli</b>  Suomi
<b>Huomautus (huomautukset liitteistä)</b>	
<b>Ohjaavan opettajan nimi</b>  Mika Ruponen	<b>Opinnäytetyön toimeksiantaja</b>  Insinööri Studio Oy

## DESCRIPTION

	<b>Date of the bachelor's thesis</b>  20.5.2016
<b>Author(s)</b> Valtteri Stenholm	<b>Degree programme and option</b> Building services
<b>Name of the bachelor's thesis</b>  Survey of HVAC-automation possibilities in Etelä-Kymenlaakso Vocational College	
<b>Abstract</b> Viewing current status of HVAC-systems and changing desired settings of them anytime and anywhere is made possible by remote management of building automation. The aim of this thesis was to examine different methods to achieve remote management of Etelä-Kymenlaakso Vocational College's HVAC systems.  Variety of different equipment and software available was rather extensive despite the limitations that were made. For this particular reason this thesis will mainly focus on the general level of remote control. Wide range study of computer communication standards and protocols of Ekami HVAC-systems was done for this study. Interviews were conducted to identify specialties of current HVAC-automation systems and also to examine a number of options to implement a viable solution to remote control building automation. In addition, the Ekami HVAC automation systems were surveyed. This allowed the making of a topology chart that shows the essential parts of current device structure.  As the research progressed it became clear that there are various remote control products on the market. Many of them enabled combining with each other, which made the amount of possible solutions quite high. Sampling was rather extensive, although available resources were limited.  The goal of this thesis was achieved as three different solutions were chosen for closer examination. The first being software based TeamViewer, which enables direct remote control of monitoring computers. The second and the third were centralized solutions that would require comprehensive renovations to current HVAC automation systems. To ensure long-term functionality, client should meet with different professionals to select the most suitable solution.	
<b>Subject headings, (keywords)</b>  HVAC automation, remote control, remote connection, BACnet, Modbus	
<b>Pages</b> 44+2	<b>Language</b> Finnish
<b>Remarks, notes on appendices</b>  	
<b>Tutor</b>  Mika Ruponen	<b>Bachelor's thesis assigned by</b>  Insinööri Studio Oy

# SISÄLTÖ

1	JOHDANTO .....	1
2	RAKENNUSAUTOMAATIO .....	1
3	VIESTINTÄPROTOKOLLAT .....	3
3.1	OSI- ja TCP/IP-mallit .....	3
3.2	Kohteen automaatioarkkitehtuurit .....	5
3.2.1	ModBus .....	5
3.2.2	BACnet .....	8
4	TYÖN LÄHTÖKOHDAT .....	10
4.1	Ekamin automaatiojärjestelmien topologia .....	11
4.2	Ekamin Windos-pohjaisten järjestelmien tietoturva.....	13
5	MAHDOLLISET ETÄHALLINTAVAIHTOEHDOT .....	15
5.1	Valvomotietokoneen etähallinta .....	15
5.1.1	Tietokoneen etähallinta ohjelmistolla .....	16
5.1.2	Tietokoneen etähallinta KVM-laitteella .....	17
5.1.3	Valvomotietokoneen etähallinta ulkoisella Lock-verkkolaitteella ..	19
5.2	Yksittäisen alakeskuksen etähallinta .....	20
5.3	Koko LVI-automaation päivittäminen etähallintaa tukevaksi .....	23
5.3.1	Citect SCADA 7.20 Web-server .....	26
5.3.2	CentralLine ARENA AX .....	27
5.4	Yhteenvedo etähallintavaihtoehtoista .....	29
6	TOTEUTUSKELPOISTEN VAIHTOEHTOJEN KUSTANNUSARVIOT.....	30
6.1	TeamViewer .....	30
6.2	Citect Web-server ja ARENA AX.....	32
7	POHDINTA .....	33
8	YHTEENVETO .....	35
	LIITTEET	
	1 Ekamin LVI-automaation nykyinen topologia	
	2 Ekamin LVI-automaation topologiaehdotus	

## LYHENNELUETTELO

EKAMI	Etelä-Kymenlaakson ammattiopisto
OSI	Open system Interconnections, Kuvaa tiedonsiirto protokollien yhdistelmän seitsemässä eri kerroksessa
TCP	Transmission Control Protocol on tietoa pilkkova, kuljuksesta huolehtiva ja tiedon perillä kokoava protokolla
TCP/IP	Tiedonsiirtoprotokollien yhdistelmä
IP	Internet Protocol, verkkolaitteen identifioimiseen käytetty numerosarja
ISO	International Organization for Standardization eli kansainvälinen standardointijärjestö
ASCII	American Standard Code for Information on 7-bittinen tietokonemerkistö
DHCP	Dynamic Host Configuration Protocol, jakaa IP-osoitteita lähiverkon laitteille
Modbus	Isäntä/renki tyyppinen automaatioväyläteknikka
BACnet	Useita viestintätapoja tukeva automaatioväyläteknikka
RJ45/8P8C	Tietoliikenneliitin
VAK	Rakennusautomaatiossa käytetty valvonta-alakeskus
SCADA	Supervisory Control and Data Acquisition eli hallinta ja tiedonkeruu
MBAP	Modbus Application header, Modbus/TCP viestin raami
ADU	Application Data Unit, Valmis Modbus RTU/ASCII viesti
PDU	Protocol Data Unit, Modbus viestin asiasisältö
KVM	Keyboard, video, mouse, Fyysinen PC:n etähallintaan käytetty laite, joka yhdistetään tietokoneen takaliittimiin
RTU	Remote Terminal Unit
UDP	User Datagram Protocol, yhteydetön viestintäprotokolla
Unit-ID	Modbus-laitteen identifiointitunnus
HMI	Human-machine interface, Ihmisen ja koneen välinen rajapinta
BBMD	BACnet Broadcast Management Device, Laite, joka vastaanottaa ja lähettää viestejä BACnet/IP verkkojen välillä

IoT

Internet of Things, Esineiden internet eli internetin kautta yhdistetyt laitteet, jotka tarjoavat informaatiota toisille laitteille ja käyttäjille

RS-232/485

Vanhoja mutta yleisesti käytössä olevia tietoliikenne väyliä

## 1 JOHDANTO

Etähallinta voidaan määritellä tavanomaista käyttöympäristöä kauempaa tapahtuvana kahden laitteen tai ohjelman välisenä tiedonsiirtona, jonka avulla ohjaava osapuoli hallinnoi toista vastaanottavaa osapuolta. Yksinkertaisimmillaan etähallinta on esimerkiksi television ohjaamista kaukosäätimellä. Suoraa näköyhteyttä vaativa kaukosäädin voidaan nykyään myös korvata internetin kautta yhdistetyllä mobiililaitteella, jonka avulla television voi ohjelmoida tallentamaan suosikkiohjelmaa esimerkiksi työpaikalta käsin. Kasvavana trendinä onkin niin sanottu IoT eli esineiden internet, jossa aikaisemmin yksittäiset laitteet yhdistetään toisiinsa internetin välityksellä tarjoamaan tietoaan sekä palveluitaan verkon muille laitteille ja käyttäjille. Myös rakennusautomaatio on osa tätä kasvavaa murrosta. Tämä näkyy muun muassa etähallintaratkaisuna, joka mahdollistaa automaatiojärjestelmien tuottaman informaation hyödyntämisen sekä järjestelmän toimintojen muokkaamisen ajasta tai paikasta riippumatta.

Tämän opinnäytetyön tarkoituksena onkin selvittää, minkä tyyppisiä LVI-automaation etähallintaan tarkoitettuja ratkaisuja on olemassa, kuinka ne eroavat toisistaan sekä kuinka niitä voidaan käytännössä hyödyntää neljässä Etelä-Kymenlaakson ammattiotiston eli Ekamin kampuksessa, joiden LVI-automaatiojärjestelmien etähallintamahdollisuuksia halutaan kartoittaa. Vaihtoehtojen tulisi mahdollistaa kampusten henkilökunnan lisäksi Ekamin yhteistyökumppaneille luotettava etähallintayhteys.

Työn tilaajana toimii Insinööri Studio Oy, joka on kotkalainen LVIS- ja arkkitehtipalveluja tarjoava suunnittelutoimisto. Studion tarkoituksena on auttaa Ekamin kiinteistönvalvontaa LVI-järjestelmien seuraamisessa ja taata niiden suunnitelmien mukainen sekä mahdollisimman energiataloudellinen toiminta.

## 2 RAKENNUSAUTOMAATIO

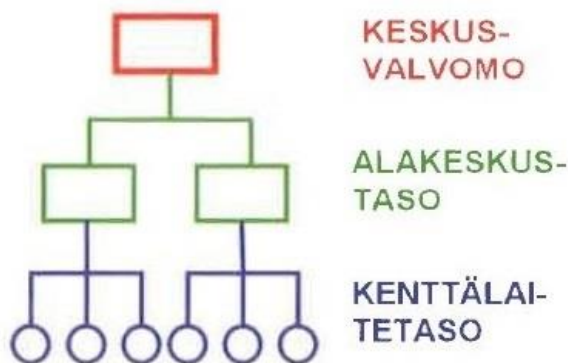
Rakennusautomaatiojärjestelmät jaetaan perinteisesti keskitettyihin ja hajautettuihin järjestelmiin. Kuvan 1 tapaan keskitetty järjestelmä on usein kolmiportainen, jossa hierarkiassa ylempänä oleva laite määrää aina alemman tason laitteiden toiminnan. Tämän järjestelmän alin eli kenttäväyläkerros yhdistää kenttälaitteet sekä niiden hal-

linnoimisesta vastaavat valvonta-alakeskukset eli VAK:it. Toinen eli automaatiokerros yhdistää puolestaan edellä mainitut alakeskukset ja paikalliset valvomokoneet toisiinsa. Ylimpänä kerroksena pidetään niin sanottua hallinnointikerrosta, joka koostuu keskusvalvomosta ja etähallinnan mahdollistavista koneista kuten palvelimista.

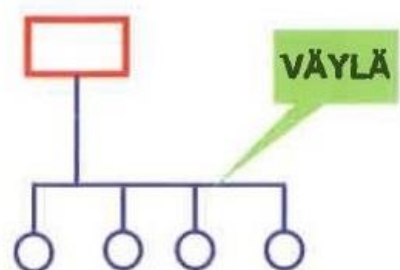
Hajautetussa järjestelmässä jokainen laite omaa hieman prosessointikykyä. Näin yksittäinen laite voi itsenäisesti suorittaa omaa tehtävästään ilman ylemmän tason ohjausta. Jotta järjestelmän suorituskyky säilyisi, voidaan suurissa rakennuksissa järjestelmä jakaa pienempiin osiin esimerkiksi LonWorks-verkossa reitittimellä tai vastaavasti EIB-verkossa linja- ja alueliittimillä. Tällöin paikallisen yksikön viestit eivät näy turhaan muille järjestelmän laitteille. /1, s. 16-20./

Keskitettyjä järjestelmiä on perinteisesti käytetty LVI-laitteiden kuten lämmityksen ja ilmastoinnin ohjaamiseen, jossa ohjattavat laitteet ovat lähellä toisiaan. Hajautettua järjestelmää käytetään useimmiten valaistuksen ohjaamiseen, sillä ohjattavat laitteet voivat olla kaukana toisistaan. /1, s. 16-20./

#### KESKITETTY JÄRJESTELMÄ



#### HAJAUTETTU JÄRJESTELMÄ



**KUVA 1. Keskitetty ja hajautettu rakennusautomaatiojärjestelmä /1, s.7./**

Rakennusautomaatiokäsike kattaakin siis koko järjestelmän fyysisistä kenttälaitteista eri väyläprotokolliin ja niistä aina internetin välityksellä yhteydessä olevaan mobiililaitteeseen asti.



Aiheen laajuudesta johtuen tässä työssä käsitelläänkin lähinnä hallinto- ja automaatiotason välisiä ratkaisuja. Tämän lisäksi jotkin etähallintaa mahdollistavat järjestelyt vaativat kuitenkin kaikkien järjestelmätasojen huomioimista. Kaikki ehdotukset ovat toteutettavissa siis yleisellä tasolla, mutta kattavaa LVI-automaatiosuunnitelmaa tehtäessä on aina kuitenkin huomioitava jokaisen järjestelmän sanelemat yksityiskohdat saumattoman toimivuuden takaamiseksi.

Uudistusten vaatimaa tietoturvaa tarkastellaan tässä työssä Ekamin Windows-pohjaisille järjestelmille asettamien vähimmäisvaatimusten mukaisesti. LVI-automaatiojärjestelmien tietoturvan yksityiskohtaisempi tarkastelu rajataan tämän insinööriyön ulkopuolelle.

### **3 VIESTINTÄPROTOKOLLAT**

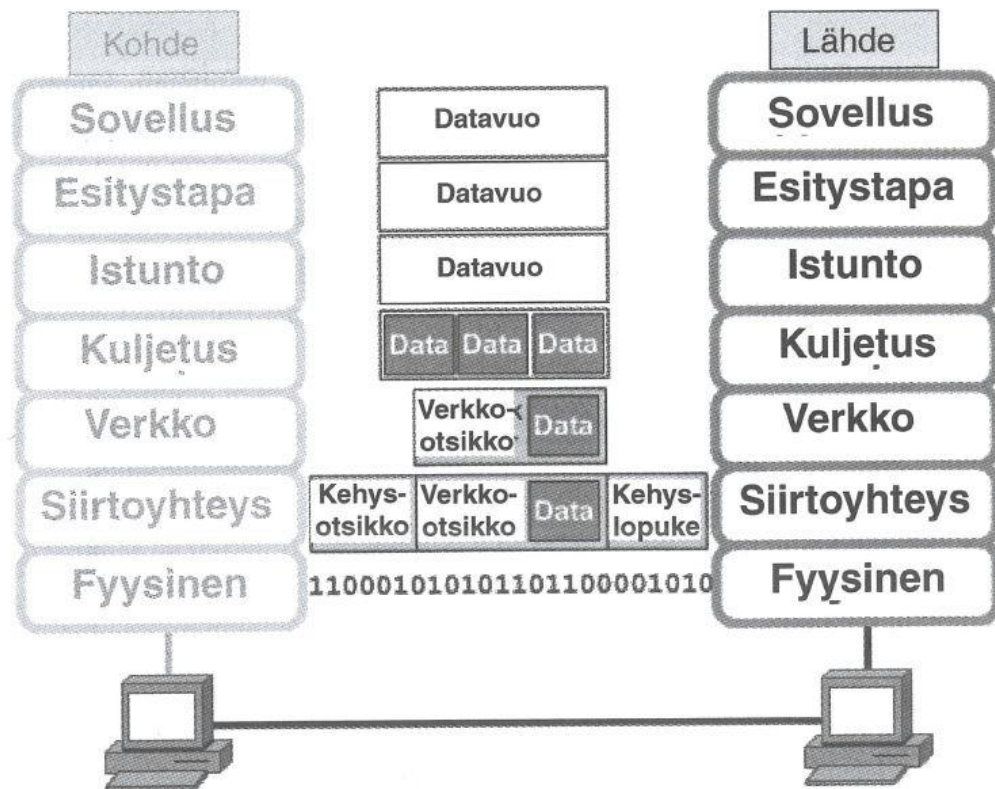
Jos kaksi toisilleen viestivää ihmistä puhuvat eri kieltä, on varsin selvää, että vastaanottavan henkilön kyky ymmärtää puhujan viestiä on heikko, ellei olematon. Samanlainen ongelma pätee myös ihmisten tuottamissa laitteissa ja ohjelmistoissa. Tätä ongelmaa varten ovat ohjelmistovalmistajat kehittäneet joukon yhteisiä sääntöjä, jotka muodostavat niin sanottuja viestintäprotokollia. Näistä suosituimmat on puolestaan hyväksytty kansainvälisiksi standardeiksi, mikä on mahdollistanut suurtenkin tietoverkkojen luomisen eri valmistajien laitteilla.

#### **3.1 OSI- ja TCP/IP-mallit**

Jotta verkkojen suunnittelijat voisivat toteuttaa toisiinsa yhteensopivia järjestelmiä, ISO eli International Organization for Standardization julkaisi vuonna 1984 niin sanotun OSI-viitemallin. Sen tarkoitus on havainnollistaa, kuinka data kulkee sovellustasolta aina fyysiselle kerrokselle asti. Kyseinen malli muodostuu seitsemästä eri kerroksesta, joista jokainen kerros käsittelee saamansa tiedon hieman eri tavalla ja lähettää prosessoidun tiedon eteenpäin seuraavalle tasolle. /1, s. 79; 2, s. 45-54./

Yksinkertaistetusti malli etenee seuraavanlaisesti. Ensimmäiset kolme ylintä OSI:n kerrosta sovellus-, esitystapa- ja istuntokerros valmistelevat datan lähetystä varten luomalla yhtenäisen rakenteen siirtoa varten. Tämän jälkeen kuljetuskerros pilkkoo saamansa datan pienemmiksi helpommin lähetettävissä oleviksi yksiköiksi, joita kut-

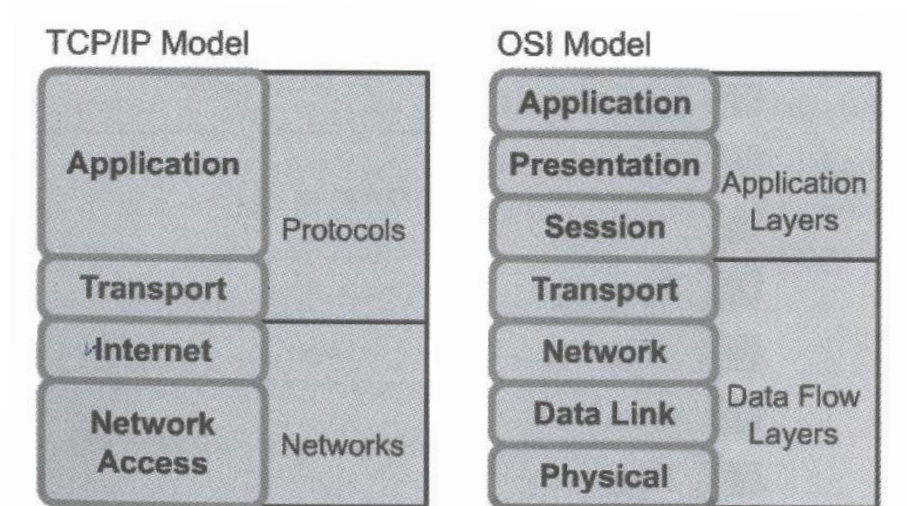
sutaan segmenteiksi. Jos lähetetty data ei jostain syystä saavu perille, on huomattavasti tehokkaampaa lähettää vain puuttuva paketti kuin koko tiedostoa. Pilkottu tiedosto mahdollistaa myös monen samanaikaisen tiedoston lähettämisen, kun koko kaistaa ei ole varattuna yhden suuren tiedoston takia. Kuljetuskerros antaa segmenteille myös yksilöllisen järjestysnumeron, jotta vastaanottaja voi koota lähetetyn viestin oikeassa järjestyksessä. Verkkokerros puolestaan kapseloi segmentin muodostaakseen paketin, joka sisältää kohde- ja lähdeverkon loogiset IP-osoitteet. Tämän jälkeen siirtoyhteyskerros muodostaa kapselille kehyksen, joka sisältää fyysisten lähde- ja kohdelaitteen MAC-osoitteet. Lopuksi siirtoyhteyskerros lähettää datan binäärimuotoisina ykkösinä ja nollina fyysisen siirtomedian kautta. Kuvassa 2 esitetään, kuinka data siirtyy kerrokselta toiselle edellä mainitun prosessin tapaan. /2, s. 51-69; 1, s. 79-87./



**KUVA 2. Informaatio kapseloidaan lähetystä varten /2, s. 59/**

Vaikka OSI-malli tarkoitettiin lähinnä viitteelliseksi ohjeeksi, käyttävät monet nykypäivän viestintästandardit ainakin osaa sen seitsemän kerroksisesta rakenteesta. Tunnetuin näistä lienee TCP/IP-standardi, joka on yksi laajimmin levinneistä viestintäprotokollista. Koska TCP/IP-protokollat ovat internetin standardeja, ovat ne yhteensopivuuden takia levinneet suurimpaan osaan nykypäivän verkkoon liitettävistä laitteista, joihin sisältyvät myös uudet rakennusautomaatiojärjestelmät. /2, s.64-69./

Kuvasta 3 nähdään, kuinka monesta yhteneväisyydestä huolimatta TCP/IP- ja OSI-mallit eroavat toisistaan. TCP/IP käytännössä tiivistää useiden kerrosten toimintoja samalle tasolle, jolloin verkkokerros huolehtii esimerkiksi siirtoyhteys- ja fyysisen tason toiminnoista. /2, s. 67./



**KUVA 3. OSI- ja TCP/IP-mallin vertailu. /2, s. 67/**

### 3.2 Kohteen automaatioarkkitehtuurit

Ekamin LVI-automaatiojärjestelmät ovat vuosien saatossa käyneet läpi lukuisia muutoksia ja lisäyksiä. Pääosin kampusten järjestelmät koostuvat Modbus- ja BACnet-protokollaa käyttävistä laitteista. Tästä johtuen muita erittäin vanhoja ja vähäisissä määrin esiintyviä laitteistoarkkitehtuureja ei tulevissa kappaleissa käsitellä.

#### 3.2.1 ModBus

Modbus on alun perin Modicon Oy:n vuonna 1979 julkistama automaatioprotokolla. Nykyään Modbus on avoin standardi, jonka kehittämisestä vastaa valmistajista riippumaton Modbus Organization. Modbus on iästään huolimatta etenkin Euroopassa suosittu LVI-automaatioväylä, jota tukee huomattava suuri määrä laitteistovalmistajia. /3, s.3-4; 1, s. 243./

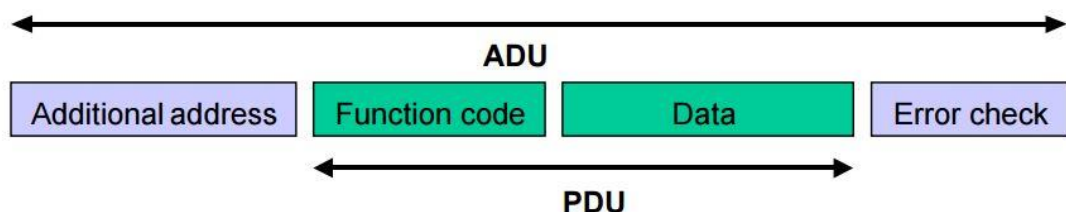
Modbus-standardista on myös ehditty julkaista jo useampia toisistaan eroavia versioita, kuten Modbus/RTU, Modbus ASCII, Modbus plus ja Modbus/TCP. Näistä kolme ensimmäistä ovat parikaapelia käyttäviä viestintämuotoja, josta RTU on standardin

mukaan suositeltava lähetysmuoto suuremman informaatiotiheydensä takia. Modbus/TCP on nimensä mukaisesti TCP/IP-standardien kanssa yhteensopiva versio, joka mahdollistaa Modbus-viestien lähettämisen IP-pohjaisen verkon yli. /4, s. 5-12; 1, s.243-246./

Modbusin toiminta perustuu niin sanottuun master - slave-periaatteeseen, jota voidaan suomeksi verrata isäntä - renki-suhteeseen. Kaikista Modbus-väylään kytketyistä laitteista vain isäntä voi lähettää toimintakäskyjä muille saman verkon laitteille. Renki puolestaan kuuntelee Modbus-väylää ja tarvittaessa vastaa isännän kyselyihin. Toisin kuin Modbus/TCP-protokolla perinteinen RTU- ja ASCII-protokolla mahdollistaa vain yhden samanaikaisen yhteyden isännän kanssa. Tämä rajoittaa RS-232- ja RS-485-väylää käyttävien ratkaisujen viestintäkapasiteettia, jolloin suurissa järjestelmissä voi esiintyä pientä viivettä. /4, s. 5-19; 1, s. 244-246; 5./

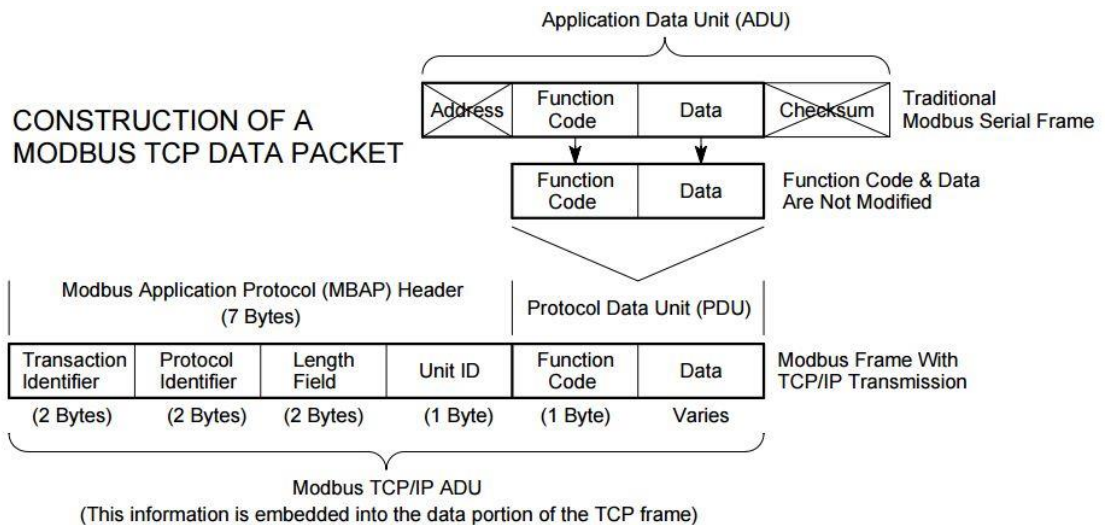
Kuvassa 4 näkyy Protocol Data Unit eli PDU. Se on Modbus-viestin ydin, joka koostuu funktiokoodista ja sitä täydentävästä data-osiosta. Näistä funktiokoodi on isännän lähettämä toimenpidekäsky, joka määrittelee rengille sille osoitetun tehtävän. Dataosio puolestaan sisältää toimenpiteeseen liittyvän lisätiedon tai vaihtoehtoisesti rengin lähettämän tiedon isännän kyselyyn. /6, s.2-6; 4, s. 8-10./

Jotta viesti voidaan lähettää oikealle laitteelle, lisätään PDU:n ympärille vastaanottavan laitteen yksilöllinen osoite. Modbus-järjestelmän osoiteavaruus kattaa kaiken kaikkiaan 256 eri osoitetta. Näistä osoite 0 on tarkoitettu yleiseksi lähetysosoitteeksi, jolloin kaikki järjestelmän laitteet saavat saman viestin. Yksittäisille reengeille tarkoitettuja osoitteita ovat 1-247. Loput kahdeksan ovat protokollan kehittäjille varattuja osoitetta. Modbus-viestin loppuun lisätään vielä virheentarkistusosio, jotta perille saapuneen viestin eheys voidaan varmistaa. Tätä edellä mainittua kokonaisuutta kutsutaan ADU:ksi eli Application Data Unitiksi. /4, s. 7-8; 7, s. 4./



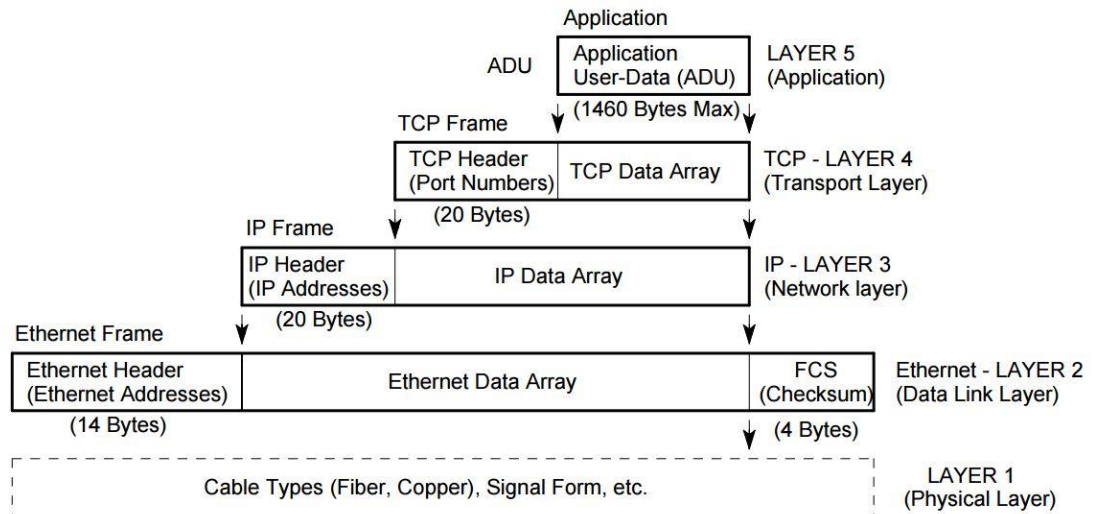
**KUVA 4. RTU- ja ASCII-tyyppinen Modbus-viesti /6, s. 4/**

PDU on käytetystä Modbus-protokollasta riippumaton yksikkö. Toisin sanoen Modbus/RTU-viesti voidaan lähettää internetin yli muuttamalla sitä ympäröivää kehystä kunkin viestintästandardin vaatimusten mukaisiksi. Modbus-viestin ydinsanoma pysyy siis samanlaisena riippumatta käytetystä viestintämediasta. Kuva 5 havainnollistaa, kuinka Modbus/RTU-viestin kehys muuttuu, kun se lähetetään TCP/IP-verkon kautta. /3, s. 3-5; 6, s.3-6./



**KUVA 5. Modbus/TCP-tunniste MBAP eli Modbus Application header /3, s. 4/**

Kun Modbus/RTU muunnetaan Modbus/TCP-muotoon, RTU:n käyttämä kehys vaihdetaan Modbus/TCP:n kehykseksi. MBAP-kehys sisältää viestitunnisteen, käytettävän protokollan tunnisteen, viestin pituus -tunnisteen ja kohdelaitteen tunnisteen, joka vastaa RTU-viestin laiteosoitetta. RTU-kehyksestä poiketen MBAP ei sisällä omaa virheentarkistusosiota, vaan virheentarkastelu tapahtuu TCP/IP-protokollan mukana. Edellä mainittu tapahtuma on havainnollistettu kuvissa 5 ja 6. /3, s. 3-5; 6, s.3-6./



**KUVA 6. Modbus-viestin paketoiminen TCP/IP-standardin mukaiseksi /3, s. 11/**

Kun Modbus-viesti on saanut oikean tyyppisen MBAP-kehiksen, paketoivat TCP/IP-protokollan tasot lähetettävän paketin, kuten minkä tahansa muun internetin yli lähetettävän viestin. /3, s.11./

Koska Modbus/TCP-viesti voi sisältää IP-osoitteen lisäksi RTU-tyylisen laitetunnisteen, ei jokaiselle laitteelle tarvitse omaa IP-osoitetta, vaan viesti voidaan lähettää IP-osoitteen omaavalle muuntimelle. Muunnin puolestaan ohjaa viestin RTU-pohjaisen alaverkon laitteelle unit-ID:n avulla. /3, s. 26./

Modbus/TCP mahdollistaa siis esimerkiksi olemassa olevan 10Base-T tai 100Base-TX-tietoliikennekaapeloinnin käyttämistä rakennusautomaation tarpeisiin. Kommunikoivat laitteet voivat olla myös huomattavan etäisyyden päässä toisistaan.

### 3.2.2 BACnet

Vuonna 1995 ASHRAE eli American Society of Heating, Refrigerating and Air-Conditioning Engineers julkaisi oman automaatioprotokollan nimeltään BACnet, joka tulee sanoista Building Automation and Control Network. Myöhemmin samana vuonna American National Standards Institute ANSI hyväksyi BACnetin yleiseksi automaatiostandardiksi. /8./

BACnet-viesti koostuu aina Application Protocol Data Unitista eli APDU:sta, joka sisältää siirrettävän datan. APDU:n lisäksi viestiin liitetään NPCI, joka voi sisältää



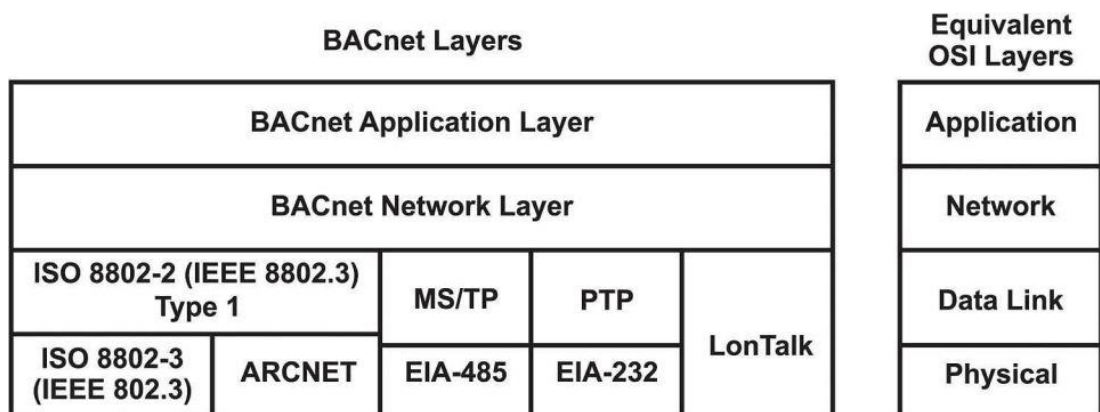
reititystietojen lisäksi viestin prioriteetin ja laitetunnisteen. Lähetystavasta riippuen voi kyseinen viesti saada vielä muita viestin reititykseen vaikuttavia kehyksiä. Kuvassa 7. näkyy yksinkertaistettu BACnet-viestin rakenne. /9, s. 2./



**KUVA 7. BACnet –viestin rakenne /9, s. 2/**

Kuvasta 8 nähdään puolestaan BACnet-protokollan käyttämät OSI-mallin tasot. Ylimpänä näistä toimi Application Layer, joka huolehtii korkean tason toiminnoista kuten viestien aikakatkaisun tarvitsemista ajastimista sekä laitteen toimintojen muuttamisen niin sanotuiksi BACnet-objekteiksi. Objektit ovat kokoelmia laitteen ominaisuuksista, joita voi olla esimerkiksi fyysiset mittausarvot taikka abstraktit asiat kuten laskujen tulokset. Näiden lisäksi jokaisella objektilla tulee olla pakolliset tunnistetiedot joita ovat Object\_Identifyer, Object\_Name ja Object Type. BACnet-standardi määrittelee 23 perusobjektia yleisimmille toiminnoille. Tämän lisäksi laitevalmistajat voivat tarvittaessa luoda omia objekteja, jos virallisista objekteista ei löydy tarvittavia toimintoja. /8, s. 17-21./

Sovellustason jälkeen tulee Network Layer eli verkkokerros, joka huolehtii pakettien toimituksesta eri BACnet-verkkojen välillä. Lopuksi siirtoyhteys- ja fyysinen kerros välittävät viestit verkossa olevien laitteiden välillä. BACnet mahdollistaa viiden eri tiedonsiirtotavan käytön. Näitä ovat ARCNET, PTP, LonTalk, MS/TP sekä internet. / 9, s. 1; 8, s.10./



**KUVA 8. BACnet-protokollan tukemat viestintävaihtoehdot / 9, s. 1/**

Kun BACnet-järjestelmään yhdistetään eri tiedonsiirtotapoja käyttäviä laitteita, tarvitaan verkkojen välille BACnet router, joka toimii yhdyskäytävänä verkkojen välillä. Kyseistä laitetta ei pidä kuitenkaan sekoittaa Gateway-muuntimeen, joka on puolestaan tarkoitettu kääntäjäksi eri protokollien välille. / 9, s. 1./

Internetiin perustuva BACnet-järjestelmä tukee suoraan kahden eri verkon välistä unicast eli laitteelta laitteelle tapahtuva tiedonvälitystä. Tämän vastakohta eli broadcast, jossa kaikki samassa verkossa olevat käyttäjät vastaanottavat saman viestin, ei ole mahdollista, koska verkkoja yhdistävät reitittimet eivät pysty välittämään yleisesti lähetettyjä viestejä. Jotta verkkojen välinen broadcast-viestien lähetys olisi mahdollista, voidaan molempiin verkkoihin lisätä niin sanottu BBMD eli BACnet Broadcast Management Device. Jos ensimmäisen verkon laite haluaa lähettää yleisen viestin toiseen verkkoon lähettää se viestinsä oman verkkonsa BBMD-laitteelle. Tämä puolestaan lähettää viestinsä toisen verkon vastaavalle laitteelle BBMD-laitteelle, joka omassa verkossaan lähettää ensimmäisen verkon laitteen viestin kaikille yleisenä broadcast-viestinä. /10, s. 6-11./

BACnet on monipuolinen automaatiostandardi, joka tukee verrattain useaa viestintämuotoa. Se tarjoaa myös helppoa yhdistettävyyttä muihin automaatiostandardeihin, jotka tarjoavat muun muassa mahdollisuuden valaistuksen hallintaa.

#### **4 TYÖN LÄHTÖKOHDAT**

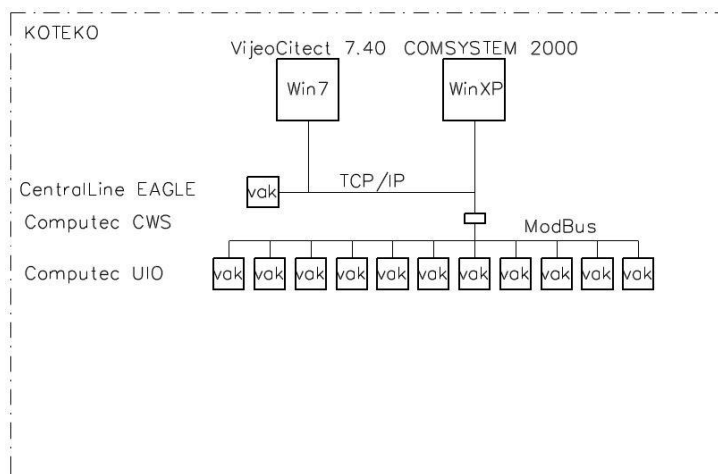
Etelä-Kymenlaakson ammattiopistolla on neljä toimipistettä, joista kolme sijaitsee Kotkassa ja yksi Haminassa. Kotkan toimipisteet ovat Katariinan kampus, Kotekon kampus ja Malmingin kampus sekä Haminassa nimensä mukaisesti Haminan kampus. Yhteensä näissä oppilaitoksissa opiskelee päivittäin noin 2800 opiskelijaa. Tämän lisäksi kampuksilla työskentelee vakituisesti myös noin 370 työntekijää. Kaikki edellä mainitut kampukset eroavat huomattavasti toisistaan rakennusten iän, koon ja käytettyjen LVI-automaatiojärjestelmien osalta.



#### 4.1 Ekamin automaatiojärjestelmien topologia

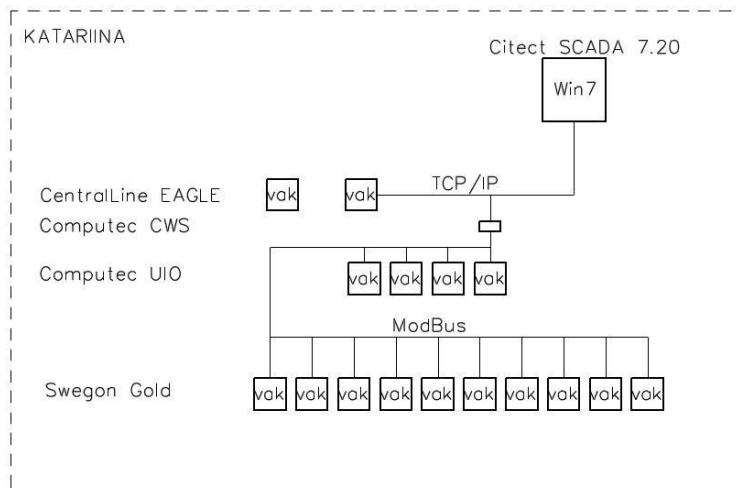
Kuvassa 9 näkyvä Kotekon LVI-automaatiojärjestelmä on rakennettu kahden valvomotietokoneen ympärille. Uudempi näistä on Windows 7 -pohjainen PC, jossa toimii VijoCitec 7.40 -valvomo-ohjelmisto. Tämä kone ohjaa BACnet-arkkitehtuuriin perustuvan Centralline EAGLE -väyläohjaimen kautta kaikkia autopuolen LVI-automaatiolaitteita sekä uudistettua auditorion ilmanvaihtokonetta. EAGLE toimii myös samalla kahden eri viestintärajapinnan välillä pakkaamalla BACnet-tyyppiset viestit TCP/IP-protokollan viesteiksi. /11; 12./

Toinen valvomotietokone on Windows XP -pohjainen PC, joka pyörittää vanhaa Citect-valvomo-ohjelmistoa. Kyseinen kone ohjaa päärakennuksen vanhoja Computec UIO 032 -alakeskuksia Computec CWS D6 DS -mediamuuntimen välityksellä. CWS toimii linkkinä kahden eri viestintäarkkitehtuurin välillä muuntaen alakeskusten Modbus/RTU-tyyppiset viestit TCP/IP-protokollamuotoon ja lähettää ne eteenpäin valvontatietokoneelle. /11; 12./



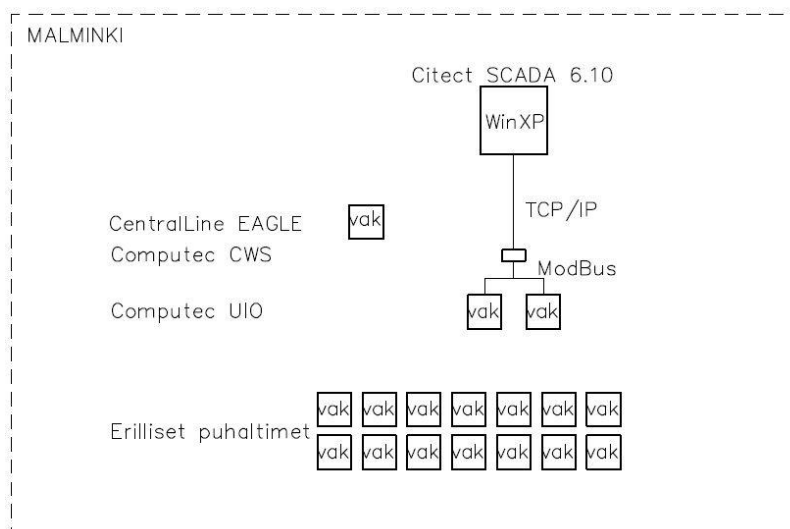
**KUVA 9. Kotekon kampuksen LVI-automaatiojärjestelmän nykytilanne**

Kuvassa 10 näkyvän Katariinan LVI-automaatiojärjestelmän valvomotietokoneena toimii Windows 7 -pohjainen PC, jossa pyörii Citect SCADA 7.20 -valvontaohjelmisto. Kyseisellä ohjelmaversiolla pystytään hallinnoimaan sekä BACnet- sekä Modbus-tyyppisiä laitteita. Kohteessa Swegon Gold -ilmanvaihtokoneet on kytketty samaan väylään Computec UIO 032 -alakeskusten kanssa, joten ne pystyvät keskustelemaan keskenään. Mediamuuntimet puolestaan toimivat samalla tavalla kuin Kotekossa. /11; 12./



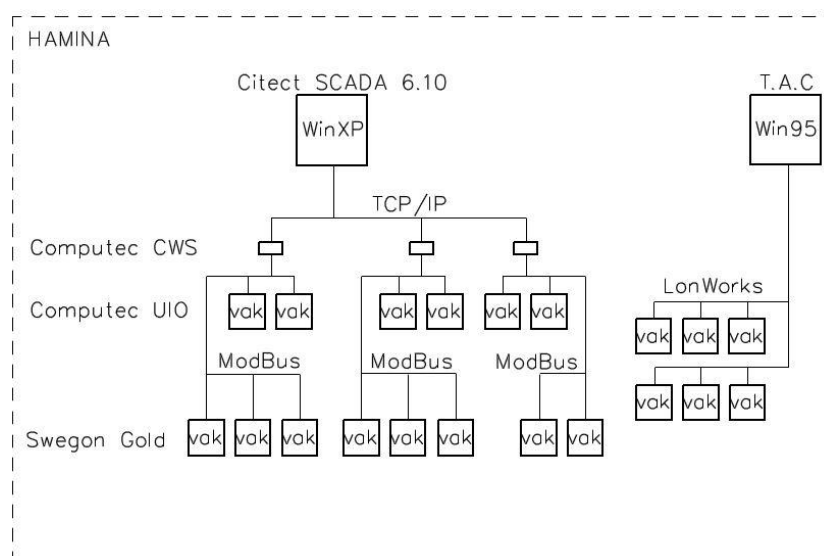
**KUVA 10. Katariinan kampuksen LVI-automaatiojärjestelmän nykytilanne**

Malmingin kampuksen vasta valmistuneen remontin yhteydessä metallipuolen hallin LVI-automaatio uudistettiin ja laitteistoarkkitehtuuri muutettiin BACnet-pohjaiseksi. Päärakennuksen automaatio jätettiin ennalleen, ja se toimii edelleen Modbus-pohjaisella ratkaisulla. Suurinta osaa Computec UIO 032 -alakeskuksista ei ole kytketty ohjausjärjestelmään, vaan ne toimivat itsenäisinä yksikköinä vailla ulkopuolista ohjausta. Kyseiset alakeskukset tullaan todennäköisesti muuttamaan BACnet-pohjaisiksi vanhojen järjestelmien rikkoutuessa. Rakennuksien ohjausjärjestelmänä toimii Windows XP -pohjaisella koneella pyörivä Citect SCADA 6.10. Mediamuunnitimet puolestaan toimivat samalla tavalla kuin Kotekossa. Edellä mainittu Malmingin järjestelmä näkyy kuvassa 11. /19; 20./



**KUVA 11. Malmingin kampuksen LVI-automaatiojärjestelmän nykytilanne**

Kuvassa 12 näkyvän Haminan kampuksen Modbus-pohjaista LVI-automaatiota ohjaa vanha Windows XP -pohjainen PC, jossa hallintajärjestelmänä pyörii Citect SCADA 6.10. Laitteistoon on suunnitteilla muutoksia, jossa valvomotietokoneen ohjelmisto päivitetäisiin Windows 7:ään ja Citect SCADA 7.20:een. Tämä mahdollistaisi nykyisin Modbus-väylässä olevien Swegon Gold -ilmanvaihtokoneiden väyläratkaisun muuttamisen BACnet-pohjaiseksi, jolloin järjestelmää nykyisin vaivaavasta kaatuilusta päästäisiin eroon. Citect-järjestelmän lisäksi osa Haminna kampuksen LVI-järjestelmistä on kytketty suoraan parikaapelilla vanhaan Windows 95-pohjaiseen valvomotietokoneeseen, jossa toimii T.A.C:n valvomo-ohjelmisto. /11; 12./



**KUVA 12. Haminan kampuksen LVI-automaatiojärjestelmän nykytilanne**

Yhtenäinen tekijä kaikissa kohteissa on, että kampusten LVI-automaatiojärjestelmiä ei ole kytketty internetiin eivätkä eri kampusten järjestelmät ole yhteydessä toisiinsa. Tämän lisäksi erityyppiset BACnet- ja Modbus-järjestelmät keskustelevat fyysisestä yhteydestä huolimatta vain saman arkkitehtuurin omaavan laitteen taikka valvomokoneiden kanssa. Esimerkiksi samassa Modbus-väylässä toimivat ComputeC UIO 032 ja Swegon Gold pystyvät tarvittaessa vaihtamaan tietoja keskenään, kun taas Modbus- ja BACnet-laitteiden välinen viestintä on toistaiseksi mahdotonta. /11; 12./

## 4.2 Ekamin Windos-pohjaisten järjestelmien tietoturva

Ekamin käytännön tietoturvasta vastaavan ICT-Kymin linjauksen mukaan kaikkien koneiden, jotka ovat Ekamin sisäverkon lisäksi yhteydessä internetiin, tulee tukea oh-

jelmistovalmistajien viimeisimpiä tietoturvapäivityksiä. Koska Ekamin tapauksessa kaikki LVI-automaation valvontatietokoneet ovat Windows-pohjaisia tarkoittaa tämä käytännössä, että kaikkien käyttöjärjestelmien on oltava vähintään Microsoftin extended supportin eli kriittisten tietoturvapäivitysten piirissä. Tämän takia nykyisellä järjestelmäkokoontamalla ei ole mahdollista liittää kaikkia valvomotietokoneita etähallinnan piiriin. Windows XP:n tuki loppui 8.4.2014, mikä siis käytännössä tarkoittaa, että vain kaksi konetta kuudesta on tällä hetkellä yhdistettävissä internetiin. /13; 14; 15./

Kuten taulukosta 1 nähdään tällä, hetkellä vanhin kriittisiä päivityksiä saava Microsoftin käyttöjärjestelmä on Windows Vista, jonka päivitykset loppuvat 11.4.2017. Selkeästi viimevuosien suosituin versio Windows-käyttöjärjestelmistä on ollut Windows 7, jonka kriittisiä päivityksiä jaetaan vuoteen 2020 asti. /15./

**TAULUKKO 1. Windows-käyttöjärjestelmien End of extended support /15 ;16./**

Käyttöjärjestelmä viimeisimmällä tietoturvapaketilla (Service Pack)	Kriittisten tietoturvapäivitysten loppuminen (End of extended support)
Windows 95 -	31.1.2001
Windows XP Service Pack 3	8.4.2014
Windows Vista Service Pack 2	11.4.2017
Windows 7 Service Pack 1	14.1.2020
Windows 8 Service Pack 8.1	10.1.2023
Windows 10 -	14.10.2025

Käyttöjärjestelmiä päivitettäessä on myös erittäin tärkeä huomioda Windows-käyttöjärjestelmien lyhyt elinkaari verrattuna LVI-automaationratkaisujen keskimääräiseen 25 vuoden elinikään.

Jos LVI-automaation valvomokoneen taikka valvomo-ohjelmistoa pyörittävän palvelimen käyttöjärjestelmäksi valitaan Windows 7, olisi koneessa käytettävien ohjelmistojen hyvä tukea Windows 10 tai vähintään Windows 8.1 -versiota pakollisia käyttöjärjestelmä päivityksiä silmälläpitäen. Työmäärän minimoimiseksi järkevin vaihtoehto olisi päivittää nykyiset käyttöjärjestelmät uusimpaan mahdolliseen versioon, jossa nykyiset tai tulevat valvomo-ohjelmistot toimivat.

Käyttöjärjestelmäpäivitysten lisäksi sisäverkon ulkopuolelle yhteydessä olevat koneet tarvitsevat oman tietoturvaohjelmiston. Ekamin tapauksessa ICT-Kymi suosittelee suomalaistaustaisen F-Secure-yhtiön tietoturvaohjelmistoa. /13; 14./

Sekä Windows-lisenssien että F-Securen tietoturvaohjelmistojen hankinta on mahdollista ulkopuoliselta toimittajalta. Toinen vaihtoehto on käyttää Ekamin omia lisenssejä valvomokoneiden ohjelmistoja päivitettäessä.

## **5 MAHDOLLISET ETÄHALLINTAVAIHTOEHDOT**

Nykyiset laite- ja ohjelmistoratkaisut tarjoavat monipuolisia vaihtoehtoja rakennusautomaation etähallintaan. Niiden avulla voidaan helposti säätää ja valvoa LVI-laitteiden toimintaa. Etähallinta voidaan toteuttaa joko hallitsemalla nykyistä järjestelmän ylintä auktoriteettia käyttävää laitetta eli valvomotietokonetta taikka päivittämällä itse rakennuksen LVI-automaatio tukemaan uusia yhteydenottomahdollisuuksia.

### **5.1 Valvomotietokoneen etähallinta**

Itse valvontakoneen etähallinta on ehdottomasti helpoin tapa saada etäyhteys tarkasteltavan kohteen automaatiojärjestelmään. Järjestelyä ei voida kuitenkaan luonnehtia puhtaaksi automaation etähallintaratkaisuksi, koska suora yhteyttä järjestelmään ei ole vaan yhteys muodostetaan välikäsiä kautta. Järjestely onkin nopea tapa kiertää itse automaatiojärjestelmän rajoitukset sekä aikaa vievät vaikeasti ratkaistavat ongelmat.

Itse valvomokoneen etähallinnan selkeänä etuna on asennuksen sekä käytön helppous. Tämän lisäksi säästytään itse automaatiolaitteiston yhteensopivuusongelmilta. Näitä ongelmia voi olla vanhenevan laitteiston yhteensopimattomuus uusien järjestelmien kanssa sekä ohjelma- että laitteistopuolella. Lisäksi erityyppisiä laitteistoarkkitehtuuria voi olla hankala integroida yhdeksi toimivaksi kokonaisuudeksi, jolloin erillisten koneiden hallinta voi olla houkutteleva ratkaisu.

Yleisellä tasolla ratkaisun ehdoton heikkous on, että läheskään kaikissa kiinteistöissä ei ole erillistä valvomokonetta, vaan alakeskus huolehtii yksin automaation ohjauksesta. Tämän lisäksi on huomioitava, että yhtä tietokonetta voi käyttää samaan aikaan

vain yksi henkilö. Esimerkiksi isossa valvomokeskuksessa voi yhden koneen takana olla useamman rakennusjärjestelmän hallintaohjelmat. Tällöin etäkäytön aikana ei paikallinen laitosmies pääse järjestelmän hallintaohjelmiin käsiksi.

### **5.1.1 Tietokoneen etähallinta ohjelmistolla**

Valvomokoneen ohjelmistopohjainen etähallinta mahdollistaa helpon etähallintamahdollisuuden internetin yli. Tällaisia ohjelmia ovat muun muassa LogMeIn ja TeamViewer. Vaihtoehtona on myös käyttää Windows-pohjaisiin käyttöjärjestelmiin sisäänrakennettua hallintaohjelmistoa.

Yksi käytetyimmistä ohjelmista on saksalaistaustainen TeamViewer-ohjelmisto, joka yhteensopivuudeltaan käy lähes kaikkiin Linux-, Windows- ja Mac Os-pohjaisiin laitteisiin. Rekisteröitymisen jälkeen ohjelmisto asennetaan molemmille käyttäjille ja ohjelma antaa kullekin laitteelle oman henkilökohtaisen ID-tunnisteen ja sisäänkirjautumissalasan. Näistä ID-tunniste on muuttumaton laitteistokohtainen tunniste, kun taas salasan saa haluttaessaan kertakäyttöiseksi.

Jotta yhteys voidaan muodostaa valvontakoneiden välille, on hallitsevan koneen tiedettävä hallittavan koneen ID sekä salasana. Kun tarvittavat tiedot on syötetty hallintakoneen ohjelmaan, voidaan yhteys muodostaa kahden koneen välille.

Ohjelmat siirtävät salausavaimensa 2048-bittisellä RSA-salauksella Saksassa sijaitsevan master-palvelimen välityksellä, joka pitää hallussa kaikkia TeamViewer-koneiden julkisia salausavaimia. Itse tietokoneiden väliseen yhteydenpitoon käytetään 256-bittistä symmetristä AES-salausta. /17, s. 3-4./

Pääkäyttäjä voi omalla lisenssillään luoda TeamViewer-koneista helposti hallintoita varten olevia ryhmiä. Tämän lisäksi ryhmille voidaan luoda niin sanotut Black- tai White list tyyppiset suodattimet, jolla voidaan tarkasti määritellä kenellä on oikeus yhdistää TeamViewer-ohjelmalla varustettuun tietokoneeseen. Esimerkiksi mustalle listalle joutunut tunnus ei voi enää yhdistää ryhmän hallittaville koneille hän vaikka tietäisikin kyseisten kohdetietokoneiden salasanat ja ID-tunnukset. Pitkällä aikavälillä ominaisuus helpottaa huomattavasti pääkäyttäjän TeamViewer-koneiden hallinnointia.

LogMeIn ja TeamViewer -ohjelmistot tukevat WoL-komentoa (Wake on LAN), jonka käyttö mahdollista (S1)uni- tai (S3)valmiustilassa olevan tietokoneen herättämisen. Kalliimmissa yleensä palvelintason ratkaisussa laitteiston voi herättää jopa täysin sammutetusta tilasta (S5). WoL-komennon toiminta perustuu verkon yli lähetettyyn heräteviestiin, johon vastaanottava kone reagoi. Jotta herätyskomento toimisi, on vastaanottavan tietokoneen verkkokortin tuettava vähintään Wake on Magic Packet -toimintoa. Asetuksen saa päälle joko tietokoneen BIOS-asetuksista tai verkkokortin omista asetuksista. Tämän lisäksi tietokoneella tulee asettaa staattinen-IP-osoite. Jotta reititin puolestaan osaisi päästää herätekomennon internetistä lähiverkkoon, on laitteelle annettava välityskomento ja avattava oikea portti. /18./

Tietokoneen etähallinta Windows-käyttöjärjestelmän sisäänrakennetulla etätyöpöytäyhteydellä eli niin sanotulla Remote Desktop -ohjelmalla on mahdollista, mutta tällöin kohde- ja ohjaavan laitteen olisi hyvä olla tietoturvan kannalta samassa verkossa. Yksi mahdollisuus on luoda suojattu yhteys kohdelaitteen paikalliseen verkkoon. Se voidaan tehdä ohjelma- taikka laitepohjaisesti.

### **5.1.2 Tietokoneen etähallinta KVM-laitteella**

KVM eli keyboard, video, mouse on tietokoneen etähallintaan tarkoitettu ulkoinen laite, joka liitetään nimensä mukaisesti tietokoneen hiiri-, näppäimistö- sekä video-porttiin. Palikka muuttaa nämä signaalit TCP/IP-protokollan mukaisiksi packageiksi, jotka voidaan lähettää Internetin yli halutulle tietokoneelle, jolla ohjaus tapahtuu. Näin saadaan yksinkertainen ja helppo rautatason etähallintaratkaisu, jolla voidaan kiertää joitain ohjelmallisen tietokoneen etähallinnan puutteita. Kuvassa 13 näkyy kahteen eri tietokoneeseen yhdistettävä KVM-laite.



**KUVA 13. Lantronix yhtiön KVM-laite /19, s. 1/**

Laitteen etuja ovat hyvä fyysinen yhteensopivuus lähes kaikkien tietokoneiden kanssa, koska tietokoneen hallintalaitteiden rajapinnat ovat PC-pohjaisissa laitteissa usein samanlaiset. Tämän lisäksi KVM-ratkaisulla voidaan ohittaa tietokoneiden ohjelmistopuolen yhteensopivuusongelmat. KVM-laite ei myöskään lisää hallittavan laitteen kuormitusta, joten kyseistä ratkaisua voidaan käyttää myös verrattain vanhoissa kokoonpanoissa.

Yhteinen kompastuskivi tietokoneiden etäohjauksen kanssa on ohjattavan koneen käynnistämisen vaikeus. Jos tietokone sammutetaan, on se usein käytävä paikanpäällä käynnistämässä uudelleen. Rautatason ratkaisun etuna on kuitenkin sen käytettävyys heti tietokoneen käynnistyessä. Toisin kuin ohjelmallisella ratkaisulla, KVM-laitteella on mahdollista päästä alemman tasoin toimintoihin, kuten tietokoneen BIOS-asetuksiin. Tämän lisäksi tietokoneen käyttäjän vaihtaminen ja sisäänkirjautuminen on mahdollista toisin kuin joissain ohjelmallisessa etäohjauksessa, jossa käyttäjän on oltava kirjaututtuna sisään, jotta etäohjausohjelma toimisi. Tällainen tilanne voi tulla vastaan esimerkiksi lyhyen sähkökatkon seurauksena, jolloin valvomotietokone käynnistyy uudestaan ja PC jää odottamaan sisäkirjautumiskomentoja.

Koska kaikki ohjelmisto ja rautapohjaiset valvomotietokoneen etähallintaratkaisut lähettävät HMI-komentojen lisäksi myös suoraa videokuvaa, vaativat ne toimiakseen verrattain nopean verkkoyhteyden hallitsevan ja hallittavan kohteen välille.



### 5.1.3 Valvomotietokoneen etähallinta ulkoisella Lock-verkkolaitteella

Tosibox Lock on suomalaistaustainen suojattujen yhteyksien luomiseen tarkoitettu laitteisto, joka koostuu Lock-vastaanottimesta ja Key USB -avaimesta. Kun avain yhdistetään tietokoneeseen, mahdollistaa se suojatun yhteyden luomisen internetin yli avainta vastaavalle Lock-laitteelle. Laite toimii siis yhdyskäytävänä kahden eri verkon välillä kuvan 14 esittämällä tavalla.



**KUVA 14. Vasemmalla Key USB -avain ja oikealla Lock-laite /20, s. 10/**

Käytännössä Lock yhdistetään fyysisesti samaan verkkoon hallittavien laitteiden kanssa. Tämän jälkeen laite tunnistaa kaikki kyseiseen sisäverkkoon kytketyt laitteet ja niihin asetetut IP-osoitteet. Lock voi vaihtoehtoisesti toimia myös DHCP-palvelimena, jolloin laite jakaa kaikille verkossa oleville laitteille vaihtuvat IP-osoitteet.

Jotta Lock-laitteeseen voidaan luoda suojattu yhteys, on sille ensin osoitettava oma avain. Luonti tapahtuu yhdistämällä Key-avain Lock-laitteen USB-porttiin. Avain ja laite vaihtavat omat julkiset avaimensa voidakseen myöhemmin tunnistaa toisensa ja vahvistaa viestien aitouden.

Kun avain ja lukko on näin sarjoitettu, voidaan laitteisto ottaa käyttöön. Yhteyden muodostamiseen vaaditaan internetiin kytketty tietokone, johon sarjoitettu USB-avain yhdistetään. Avaimen sisältämä ohjelmisto asennetaan tietokoneelle, jonka jälkeen avaimelle tulee asettaa salasana väärinkäytösten välttämiseksi. Näiden toimenpiteiden jälkeen laitteisto on periaatteessa käyttövalmis.

Lock-järjestelmään perustuvan laitteiston etuna vahvan suojauksen lisäksi on, että Lock-laite itsessään ei tarvitse kiinteää IP-osoitetta. Tavallisesti netin palveluntarjoajan antamat IPV4-osoitteet ovat vaihtuvia, jonka takia internetiin kytketyn laitteen

looginen osoite vaihtuu tietyn väliajoin. Jotta laitteeseen voidaan muodostaa yhteys verkon ulkopuolelta, on sen osoite aina tiedettävä. Lock kiertää tämän rajoituksen lähettämällä osoitetietonsa tietyin väliajoin Tosiboxin palvelimelle, joka omaa kiinteän IP-osoitteen. Lock-laitteeseen yhteyttä muodostaessa tietokone lähettää kyselyn avainta vastaavasta Lock-laitteen reititystiedoista. Saatuaan nämä tiedot tietokone voi muodostaa suoran yhteyden kyseisen Lock-laitteen kanssa. /21; 22./

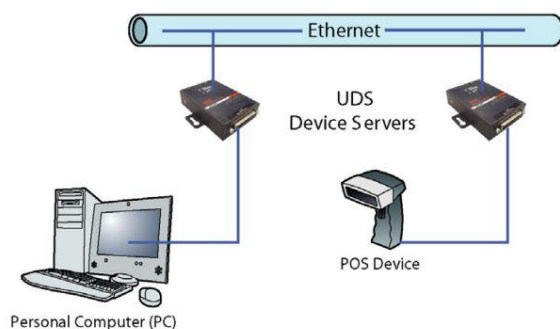
Lock-laitteeseen on mahdollista luoda lisäävaimia, jolloin useampi henkilö pääsee käsiksi lukon kautta yhdistettyyn verkkoon. Sarjoitetulla avaimella on myös mahdollista luoda oma avain Android- ja Applen IOS-mobiililaitteille Mobile Client -ohjelmalla, jolloin etähallinta onnistuu myös kännykän taikka tabletin kautta. /23; 22./

Jotta järjestelmän etähallinta olisi mahdollista, on ohjattavan laitteen omattava http-pohjainen seilainkäyttöliittymä. Yhä useampi uusi alakeskus onkin nykyään varustettu kyseisellä ominaisuudella. Etähallinta on myös mahdollista, jos rakennuksen automaatiojärjestelmä on keskitetty palvelimeen, joka mahdollistaa selainpohjaisen hallinnoinnin. Tarkemmin keskitetystä hallintaratkaisusta löytyy tämän työn kohdasta 5.3. Jos alakeskuksista tai palvelimelta ei selaintoimintoa löydy, mahdollistaa Lock-laitteisto myös perinteisen valvomotietokoneen etähallinnan. Tällöin valvontatietokoneen käyttöjärjestelmän on tuettava Windowsin omaa Remote Desktop -ominaisuutta, jonka on myös tällöin oltava kytkettynä päälle. Työpöydän etähallintaa käytettäessä samanaikaisien käyttäjien määrä on kuitenkin rajoitettu yhteen per hallittava kohde. /20, s.17./

Jos Tosiboxin Lock-järjestelmä valitaan yhteyden muodostamiseen, on Ekamin tapauksessa käytännössä kaksi vaihtoehtoa: joko jokaiselle nykyiselle valvomokoneelle hankitaan oma Lock-laite tai rakennusten yhteiselle palvelimelle hankitaan yksi yhteinen laite. /11./

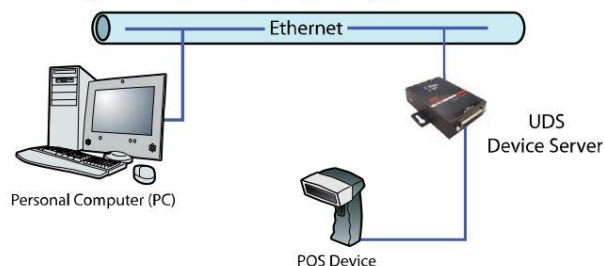
## 5.2 Yksittäisen alakeskuksen etähallinta

Lantronixin kehittämät USD1100-sarjan laitteet mahdollistavat lähes mikä tahansa COM-liitännäisten TCP/IP-standardiin sopimattomien laitteiden liittämisen verkon yli toisiinsa. Kuvassa 15 näkyy USD1100-API laitteen kytkentä mahdollisuuksia.



The Com Port Redirector software included on the product CD simplifies the integration process by extending the functionality of COM-port-based Windows™ applications. Virtual COM ports, mapped to remote device servers on the network, can replace direct serial connections.

Figure 2-2. Direct TCP/IP or Redirector Configuration



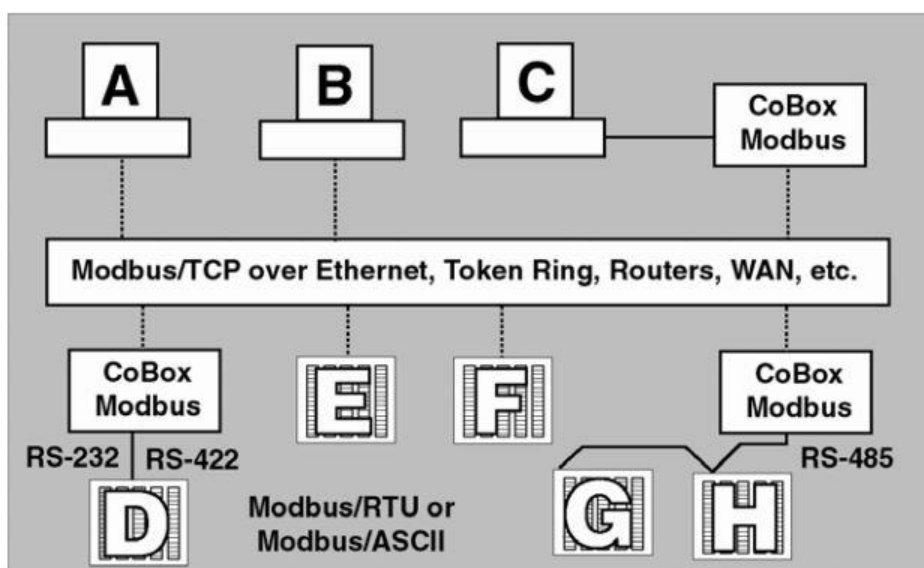
#### KUVA 15. Liitäntäehdotus USD1100-API-laitteelle /24, s. 10/

LVI-automaatioratkaisussa vanha verkkoyhteyteen kykenemätön alakeskus voidaan liittää COM1- tai COM2-portin kautta USD1100-API-muuntimeen. Laite tukee yleisimmin alakeskusten välissä tietoliikenteessä käytettyjä tiedonvälitystapoja RS-232 ja RS-485. USD1100-laitteessa alakeskuksen lähettämän signaalin data pilkotaan ja pakataan TCP-protokollan muotoon. Halutessa laitteessa voidaan käyttää myös UDP-protokollaa, mutta tällöin viestin perillemeno ei voida varmistaa. /25, s. 5-8./

Laite luo RJ45-porttiin liitetyn 10Base-T tai 100Base-TX -johdon kautta yhteyden verkon yli ennalta määriteltyihin vastaanottajien IP-osoitteisiin. Vastaanottava laite, tässä tapauksessa USD1100-API, purkaa viestin käänteisessä järjestyksessä ja lähettää lopulta viestin kohdelaitteelle. Vastaanottavana laitteena on mahdollista olla myös PC-pohjainen tietokone, joka on suoraan liitetty RJ45:n kautta samaan verkkoon lähettävän laitteen kanssa. Koska USD1100-API toiminta perustuu yleisesti internetissä käytettyihin viestintästandardeihin, voidaan yhteydenpitoon lähiverkon lisäksi käyttää myös internetiä. /25, s. 5-8; 28./

Kuvasta 16 on nähtävissä erilaisia liitännätaratkaisuja USD1100-API-laitteelle. Esimerkissä A-, B-, E- ja F-laitteet tukevat suoraan Modbus/TCP-standardia. USD1100-API mahdollistaa tavanomaisten Modbus/RTU-arkkitehtuuria käyttävien laitteiden liittämisen samaan verkkoon Modbus/TCP-laitteiden kanssa. Tässä tapauksessa laitteet D, G ja H ovat perinteisiä Modbus/RTU-arkkitehtuuria edustavia renkistatuksen omaavia laitteita. Näistä laite D on yhdistetty USD1100-IAP-muuntimeen tavanomaisella RS-232-väylällä, joka rajoittaa yhdistettävien laitteiden määrän yhteen. Tämän lisäksi Modbus/RTU rajoittaa laitteen D toimimaan ainoastaan joko isäntänä taikka renkinä. /25, s. 5-8./

Laitteet G ja H -käyttävät viestintään puolestaan RS-485-väylää, jolloin useamman laitteen liittäminen USD1100-IAP -muuntimeen on mahdollista. Ratkaisu kuitenkin rajoittaa kyseisten laitteiden toimimaan renkeinä. /25, s. 5-8./



**KUVA 16. Mahdolliset USD1100-IAP:n liitännätaratkaisut Modbus-väylään /25, s. 6/**

Järjestelmä mahdollistaa myös tavanomaisen Modbus/RTU-isännän liittämisen yhteiseen TCP-pohjaiseen järjestelmään. Kuvassa 16 tätä laitetta vastaava kirjain on C. Tässä tapauksessa laite C kohtelee kaikkia muita verkon laitteita renkeinä. Vastaavasti muut laitteet havaitsevat laitteen C isäntänä. Koska Modbus/RTU rajoittaa laitteen C toimimaan ainoastaan isäntänä, eivät suoraan Modbus/TCP:tä tukevat laitteet, kuten A, B, E ja F, voi lähettää komentoja laitteelle C. /25, s. 5-8./

Rajoituksistaan huolimatta USD1100-laitteet sopivat erityisesti tapauksiin, jossa ole-massa olevaan TCP/IP-pohjaiseen järjestelmään halutaan liittää vanhoja ennestään kytkemättömiä alakeskuksia. /21/

### 5.3 Koko LVI-automaation päivittäminen etähallintaa tukevaksi

LVI-automaatiojärjestelmän päivittäminen yhtenä kokonaisuutena toimivaksi järjestelmäksi on tulevaisuuden käytettävyyden sekä laajennuksien kannalta toimivin ja tehokkain ratkaisu. Järjestelmä rakentuisi yhden keskitetyn palvelimen ympärille, johon kaikki alakeskukset olisivat internetin kautta yhteydessä. Laitteistojen hallinta tapahtuisi webselain-pohjaisella käyttöliittymällä, joka toimisi periaatteessa missä tahansa internetiin yhdistetyssä nettiselaimella varustetussa laitteessa. Tätä vaihtoehtoa harkittaessa on kuitenkin huomioitava, että osa etenkin vanhemmista selainpohjaisista valvomo-käyttöliittymistä toimii vain Windows Internet Explorer-selaimilla. Tällöin esimerkiksi mobiililaitteiden kuten kännyköiden taikka tablettien käyttö valvomon tarkasteluun ei ole mahdollista. Modernimmat valvomo-ohjelmistot tukevat HTLM5-kieltä, jota puolestaan tukevat lähes kaikki nykyaikaiset selainohjelmistot. Tällöin myös mobiililaitteiden käyttö olisi mahdollista. On kuitenkin hyvä muistaa, että selainvalvomon käyttäminen pieneltä ruudulta voi osoittautua hankalaksi. Monia laitteita tukeva käyttöliittymä ei siis poista perinteisen valvomotietokoneen ja tarpeeksi ison näytön tarvetta. /26./

Keskitetyssä järjestelmässä käyttäjiä voi olla teoriassa rajaton määrä eikä käyttäjien lisääminen taikka poistaminen aiheuta ylimääräisiä kustannuksia. Tämän lisäksi pääkäyttäjä voi helposti hallinnoida kunkin alemman tason käyttäjän oikeuksia, joilla he voivat tehdä muutoksia järjestelmien asetuksiin. Näin varmistetaan, että kullakin käyttäjällä on hänen osaamistaan sekä käyttöoikeuttaan vastaava turvaluokitus muutosten tekemiseen. Käyttäjien helppo hallinnoiminen mahdollistaa esimerkiksi oppilastunnukset, joita voidaan hyödyntää muun muassa sähkö- ja LVI-alan koulutuksissa. Oppilastunnuksilla käyttäjä pääsee tarkastelemaan järjestelmän toimintaa siten, että kaikki muutosominaisuudet ovat poissa käytöstä. Näin eliminoidaan vahinkojen tapahtuminen ja taataan hyvä oppimisympäristö.

Toisin kuin esimerkiksi ohjelmallisesti etähallitulla koneella, etähallintaan tehty ohjelmisto tukee useaa samanaikaista käyttäjää. Näin kaikki pystyvät käyttämään järjes-

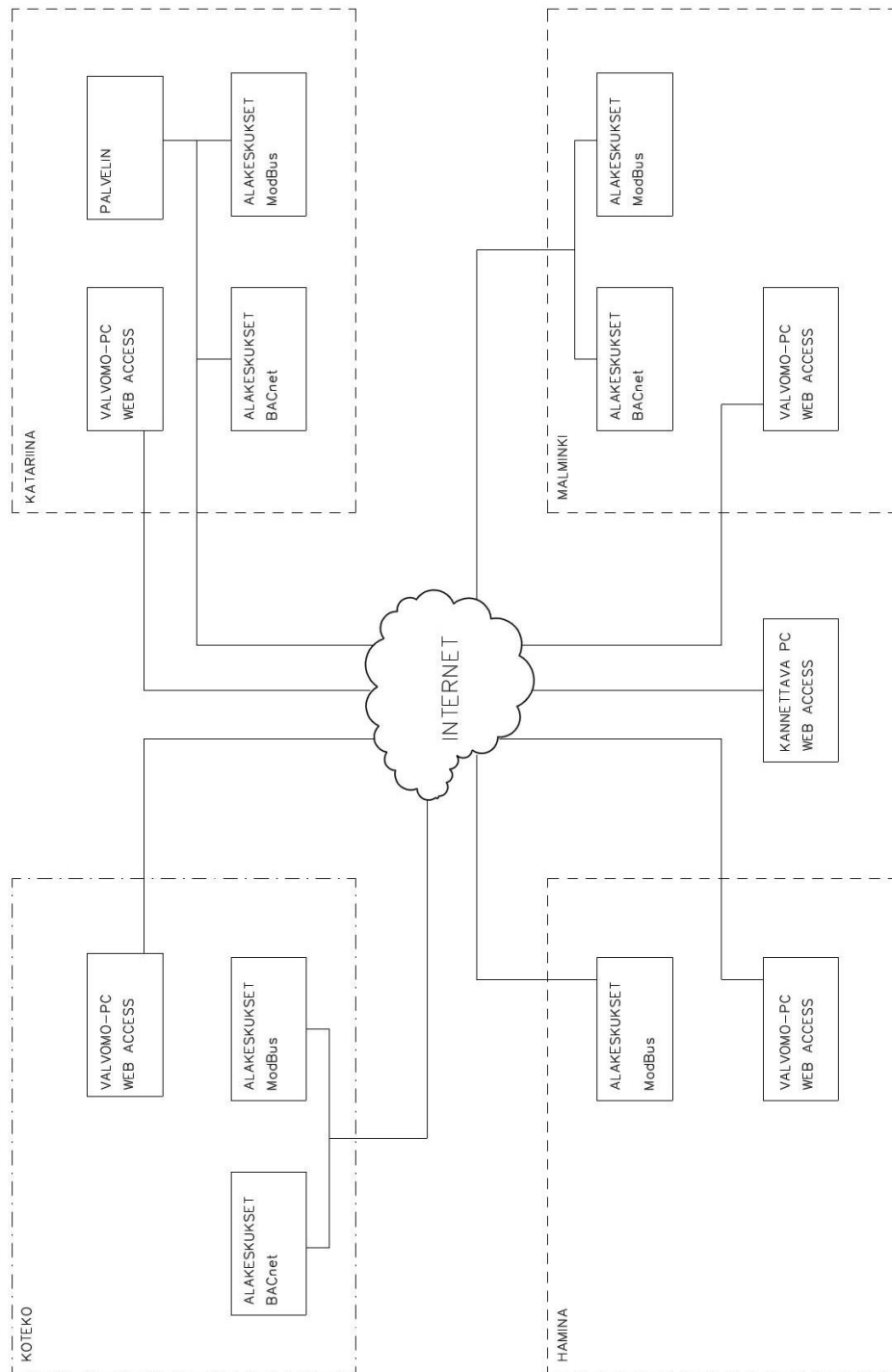
telmän toimintoja toisistaan riippumatta eivätkä useammankaan käyttäjän toimet sotke järjestelmää. Erityisesti suuremmissa laitoksissa kriittisten vikojen samanaikainen ilmaantuminen voi olla hyvinkin todennäköistä. Tällöin järjestelmän ylläpidosta vastaavan henkilön on päästävä mahdollisimman nopeasti tarkastamaan tilanneetta odottamatta etähallitun koneen vapautumista taikka muita hidastavia häiriötekijöitä.

Keskitetyn ratkaisun muita etuja ovat muun muassa yhden lisenssin hallinnoimisen, päivittämisen ja ylläpidon tehokkuus. Nykytilanteessa jokaiselle valvomokoneelle on maksettava oma lisenssi, jos järjestelmissä ilmenee päivitystarvetta. Lisäksi keskitetyssä ratkaisussa kaikkien kohteiden hallinnoiminen on mahdollista yhdeltä päätteeltä.

Keskitetyn ratkaisun heikkous on sen haavoittuvuus. Esimerkiksi sähkö- taikka tietoliikennekatkon aikana ei webvalvomoon ole mahdollista päästä. Tosin laajan ja pitkäkestoisen sähkökatkon aikana myös ohjattavat LVI-järjestelmät kuten puhaltimet ovat alhaalla, joten minkäänlainen ohjaaminen ei nykyiselläkään järjestelmällä olisi mahdollista. Palvelimia on kuitenkin mahdollista suojata sähkökatkojen aiheuttamilta ongelmilta esimerkiksi UPS-varavirtalaitteistolla. Kyseinen laitteisto takaa lyhytkestoisten katkosten aikana palvelimen tasaisen sähkönsyötön. Jos katkos kestää puolestaan odotettua pidempään, voi varavirtalaitteisto antaa palvelimelle komennon ajaa järjestelmä turvallisesti alas vielä, kun sähköä on jäljellä. Tällä ratkaisulla vähennetään järjestelmän yllättävän sammumisen aiheuttamia ongelmia.

Oheisessa kuvassa 17 on esitetty, kuinka keskitetty valvomoratkaisu toimisi. Tässä tilanteessa palvelin on sijoitettu Katariinan kampukselle ja kaikki valvomokoneet ovat vain internetyhteydellä varustettuja tietokoneita ilman omaa valvomo-ohjelmistoa. Yhteyden ottamiseksi rakennuksen LVI-automaatiojärjestelmiin on yhteys ensin luotava palvelimelle. Tämän jälkeen järjestelmään kirjaudutaan sisään ja halutut toiminnot voidaan suorittaa.

Oman palvelimen vaihtoehdoksi jotkin yritykset myyvät kokonaisvaltaista hallintapalvelua, jossa oma palvelin on korvattu palveluntarjoajan laitteistolla. Tässä tapauksessa asiakkaan LVI-automaatiolaitteisto on internetin yli yhteydessä ohjauspalvelimeen ja etähallinta hoidetaan ottamalla yhteys palveluntarjoajan palvelimeen. Palveluntarjoaja huolehtii palvelimen ylläpidosta, päivityksistä, tietoturvasta, tietojen tallennuksesta sekä käyttäjälupien hallinnoimisesta.



**KUVA 17. Ehdotus EKAMI:n LVI-automaation topologiasta, jos järjestelmä uusitaan**

Jotta yhteydenpito eri kampusten järjestelmien välillä toimisi, on kunkin kohteen LVI-automaatiojärjestelmä kytkettävä internetiin. Tämä vaatii palvelimelle joko omaa muuttumatonta IP-osoitetta tai Tosibox Lock -tyyppisen laitteen.

Jotta automaatiopalvelimeen saataisi yhteys, on sen IP-osoitteen pysyttävä aina samana. Tätä varten palveluntarjoajat myyvät erityisesti yrityksiä varten kiinteällä IP-osoitteella varustettuja internetyhteyksiä. Tämän lisäksi kertakorvauksella ja tietyllä kuukausihintaa vastaan saa useampia kiinteitä osoitteita per ostettu liittymä.

Jotta eri rakennusten laitteet pystyisivät viestimään keskenään, on jokaista rakennusta edustavan laitteen omattava muuttumaton IP-osoite. Toinen vaihtoehto on yhdistää rakennukset käyttämällä olemassa olevaa Ekamin kampusten välistä virtuaalista lähiverkkoa. Näin vain yhdessä koneessa eli palveluita ulospäin tarjoavassa palvelimessa tarvitsisi olla kiinteä IP-osoite. Kyseinen ratkaisu säästäisi pitkällä aikavälillä rahaa sekä vähäisiksi käyviä IPV4- osoitteita.

Toinen vaihtoehto on käyttää kohdassa 5.1.3 esiteltyä Tosibox Lock -laitetta, jolla muodostetaan suojattu yhteys verkkoon, jossa palvelin sijaitsee. Lock-laitteen etuna on, että se ei tarvitse kiinteää IP-osoitetta toimiakseen. Laite kiertää rajoituksen ilmoittamalla oman muuttuneen osoitteensa valmistajan omalle palvelimelle. Kun yhteys LVI-automaatiopalvelimelle halutaan luoda, kysyy yhteyttä muodostava kone Tosiboxin palvelimelta Lock-laitteen nykyisen IP-osoitteen ja yhteyden luonti on mahdollista. Tosiboxin Lock-järjestelmän etuna on myös sen kertaluontoinen hankintakustannus verrattuna kiinteän IP-osoitteen kuukausimaksuihin. /11; 23; 22./

### **5.3.1 Citect SCADA 7.20 Web-server**

Citect SCADA on Schneider electricin LVI-automaation hallintaan suunnattu ohjelmistosarja. Australialaista alkuperää oleva ohjelmisto on ollut käytössä myös suomalaisissa kohteissa. Esimerkiksi entisen Computec Oy:n tuotteet ovat käyttäneet valvontaohjelmanaan Citect-ohjelmistoa. Nykyään Citect-pohjaisia järjestelmiä saa Schneider electricin lisäksi Caverion Oy:ltä, joka yrityskauppojen myötä hankki omistukseensa Computec Oy:n.

Citect-pohjainen hallintaohjelmisto mahdollistaisi periaatteessa järjestelmän pitämisen samantapaisena ilman suurempia fyysisiä muutoksia. Toteutusvaihtoehtoja on tässä tapauksessa kaksi. Näistä ensimmäisessä kaikki laitteet olisivat siis yhteydessä yhteen palvelinkoneeseen. Tässä tapauksessa sopivaa keskuskonetta valittaessa on syytä huomioida nykyisissä valvomokoneissa toimivien lisenssien ominaisuudet. Jotta kes-



kuspalvelin pystyisi hallinnoimaan kaikkien kohteiden järjestelmiä, on siinä toimivan lisenssin tuettava kappalemäärällisesti kaikkia siihen liitettyjä laitteita. Tämän lisäksi hallintaohjelmiston versio tulee olla vähintään 7.20. Todennäköisesti tilaajalle edullisin vaihtoehto on päivittää valvomo-ohjelmisto, jonka lisenssi tukee valmiiksi mahdollisimman suurta laitekantaa. Kun eri kampusten järjestelmät tuodaan yhteen järjestelmien laitteiden käyttämät osoitetiedot tulevat todennäköisesti olemaan päällekkäisiä. Tällöin yhden kampuksen laitteisto-osoitteisto jätetään ennalleen ja muiden kampusten osalta osoitteisto uudistetaan. /27, s.1-5; 25./

Toinen vaihtoehto on pitää nykyiset valvomot ennallaan. Tällöinkin kampukset saisivat oman yhteisen LVI-automaatiopalvelimen. Palvelin olisi kuitenkin yhteydessä vain kampusta hallinnoiviin valvontatietokoneisiin, ei itse automaatiojärjestelmiin. Tällöin välttyttäisiin työläältä osoitteiston muutokselta. /27, s.1-5; 25./

Molemmissa tapauksissa internetselaimen kautta tapahtuvaa etähallinnointia varten tarvitaan joko Web Display Client, joka tukee vain Internet Explorer -selainta tai Citect Anywhere -lisenssi, joka toimii HTML5-pohjalla, jolloin kaikki modernit selaimet voivat ottaa yhteyden valvomopalvelimeen. Jokaista yhteyttä ylläpitämään tarvitaan myös Web Control Client. Pelkällä katseluominaisuudella varustettuja lisenssejä varten tarvitaan myös oma View Client. /27, s.1-5; 25./

Päivitettyinä uusimpaan valmistajan tietoturvakettiin Citect 7.20 ja sitä uudemmat ohjelmistoversiot tukevat Windows 7 sekä Windows 8.1 käyttöjärjestelmäversioita. /28, s. 2./

### **5.3.2 CentralLine ARENA AX**

CentralLine on Honeywellin omistama tytäryhtiö, joka kehittää LVI-automaatiotuotteita sekä ohjelmisto- että laitteistopuolelle. ARENA AX on Centrallinen oma valvontaohjelmisto LVI-automaatiolaitteille. Se perustuu Tridium-yhtiön omaan Niagra-ohjelmistoalustaan, joka mahdollistaa perinteisten valvontatyökalujen lisäksi selaimen kautta suoritettua etähallinnaa. /11; 12./

ARENA AX tukee pääasiassa BACnet-pohjaisia laitteita. Näiden lisäksi on järjestelmään mahdollista lisätä muita viestintäarkkitehtuureja tukevia laitteita niin sanottujen

gateway-muuntimien avulla tai hankkimalla ARENA AX-ohjelmistoon ajuri päivitys. Jotta kyseinen järjestelmä toimisi, on kampusten laitteistopuolelle tehtävä seuraavanlaiset päivitykset. /30, s. 1-4; 11; 12; 5./

Kaikki vanhat Computecin CWS:sät on vaihdettava Centrallinen Hawk-muuntimiin, jotta vanhat ModBus- laitteet kykenevät keskustelemaan ARENA AX -ohjelman kanssa. Toinen vaihtoehto on hankkia Modbus-lisäosa Arena AX -ohjelmistoon. Tämän avulla saadaan itse hallintaohjelmisto ymmärtämään Modbus-viestintää, jolloin kyseisiä viestejä ei tarvitse muuntaa BACnet-muotoon erillisellä laitteistolla. /30, s. 1-4; 11; 12; 5./

Swegon Gold -ilmanvaihtolaitteet ovat puolestaan suoraan BACnet-yhteensopivia. Ne tarvitsevat kuitenkin Centrallinen Eagle -keskuksen voidakseen olla yhteydessä talon ulkopuoliseen verkkoon. Jos rakennuksessa on jo olemassa Eagle-keskus, voidaan niitä käyttää hyödyksi liittäessä Swegon Gold -IV-koneita BACnetin kautta valvontajärjestelmään. Muutoin rakennukseen on hankittava uusi Eagle-keskus. Kuvassa 18 on esitetty eri järjestelmien mahdollistamat integraatiot ratkaisut. /30, s. 1-4; 11; 12; 5./



**KUVA 18. BACnet-protokollan liittäntämahdollisuudet /30, s. 3/**

Jotta ARENA AX -järjestelmä toimisi, on sille Citect SCADA 7.20 Web-serverin tapaan määriteltävä oma palvelin, johon kampusten LVI-automaatio on yhteydessä. Koska ARENA AX ei perustu nykyisiin valvomo-ohjelmistoihin ja niiden lisenssei-

hin, voidaan uusi LVI-automaatiopalvelin sijoittaa mihin tahansa Ekamin valvomoista. Tämän lisäksi ARENA AX tukee Windows 7, 8.1 ja 10 käyttöjärjestelmäversiota. /30, s. 1; 31./

#### **5.4 Yhteenveto etähallintavaihtoehtoista**

Ohjelmistopohjainen hallintaohjelmisto mahdollistaa yksittäisen valvomokoneen hallinnan. Samalla etähallintalupien valvonta ja seuraaminen on helppoa verrattuna muihin vaihtoehtoihin. Laitteistopohjainen KVM-ratkaisu tarjoaisi rautatason yhteyden valvomokoneisiin. Ongelmaksi muodostuu nykyisten koneiden vähäiset liitännät mahdollisuudet. Lisäksi ilman salattua yhteyttä KVM-laite sopii lähinnä lähiverkon kautta tapahtuvaan hallintaan.

Yksittäisen alakeskuksen ohjaamisen mahdollistava USD1100-API toimisi parhaiten Citect-pohjaisen hallintajärjestelmän kanssa, koska kyseinen laite käyttää kommunikointiin Modbus/TCP-pohjaisia viestejä. Tällöin muut Modbus-laitteet sekä valvomo olisivat suoraan yhteensopivia USD1100-API:n kanssa. ARENA AX saadaan ymmärtämään Modbus/TCP-viestejä lisensipäivityksen jälkeen. Tällöin järjestelmässä olisi kuitenkin edelleen kahta eri automaatioprotokollaa, mikä voi tulevaisuudessa hankaloittaa järjestelmäpäivityksiä. Tämän lisäksi vanhojen yksittäisten laitteiden lisääminen hallintajärjestelmän piiriin uudella erillisellä laitteella ei välttämättä ole taloudellisesti järkevää, koska laitekantaa uusittaessa uudet laitteet tullaan todennäköisesti liittämään suoraan olemassa olevaan hallintajärjestelmään.

Tosiboxin Lock- ja Key-laitteet mahdollistavat yksittäisten tietokoneiden suoran etähallinnan. Vaihtoehtoisesti laitetta voitaisiin käyttää kampusten yhteisen automaatiopalvelimen yhteyden luontiin. Kaikissa vaihtoehtoissa jokaiselle käyttäjälle tarvittaisiin omat USB-key-avaimet.

Koko LVI-automaation hallintajärjestelmän keskittäminen mahdollistaisi lähes kaikkien Ekamin järjestelmien seuraamisen ja säätämisen nettiselaimella. Järjestelmässä voitaisiin hyödyntää vanhaa hallintaohjelmistoa tai vaihtoehtoisesti hankkia kokonaan uusi hallintajärjestelmä.

## 6 TOTEUTUSKELPOISTEN VAIHTOEHTOJEN KUSTANNUSARVIOT

Ekamin, ICT-Kymin sekä paikallisen automaatioyrittäjä AdConSys Oy:n kanssa käytyjen keskustelujen perusteella seuraavat vaihtoehdot olisivat parhaiten toteutettavissa. On kuitenkin tärkeä ottaa huomioon, että mikään seuraavista toteutustavoista ei kata kaikkia Ekamin LVI-automaation piirissä olevia laitteita, vaan järjestelmän ulkopuolelle jää toteutustavasta riippuen muutamia LVI-järjestelmiä.

### 6.1 TeamViewer

Alkuperäisenä ajatuksena oli hankkia TeamViewer-ohjelmisto kaikkiin Ekamin kampusten valvomotietokoneisiin. Vaihtoehto olisi edullinen ja helppo väliaikaisratkaisu, kunnes itse LVI-automaatiojärjestelmä päivitettäisiin etähallintaa tukevaksi. Päivityksen jälkeen ei ohjelmasta välttämättä tulisi tarpeetonta vaan se voitaisiin siirtää muihin etähallintaa vaativiin käyttökohteisiin Ekamin sisällä. Tämän lisäksi TeamViewer-ohjelmistolla on kattava käyttöjärjestelmätuki, joten tietokoneiden päivittyminen ei olisi ongelma toisin kuin esimerkiksi KVM-ratkaisussa, jossa valvomokoneen fyysinen päivittäminen vaihtaisi nykyisin käytössä olevat vanhat liitintyypit uusiin, jolloin hallintalaitteistokin täytyisi päivittää. TeamViever ratkaisu olisi myös antanut Ekamille kokemuksia yksinkertaisesta rakennusautomaation etähallinnasta sekä mahdollistanut valittujen yhteistyökumppaneiden liittymisen etänä valvomotietokoneisiin.

Kuten kappaleessa 4.2 kerrottiin, tämän hetkisten käyttöjärjestelmien versiot eivät kuitenkaan suoraan anna mahdollisuutta asentaa ja käyttää TeamViewer-ohjelmistoa. Tämän lisäksi valvomokoneiden käyttämällä osoitteistolla ei tällä hetkellä ole mahdollista päästä Ekamin ulkopuoliseen verkkoon. Valvomokoneiden verkkoasetusten muuttaminen voi puolestaan haitata valvomokoneen kommunikointia automaatiojärjestelmän kanssa.

ICT-Kymin kanssa käytyjen keskustelujen perusteella vaihtoehtoja on kolme. Näistä ensimmäisessä automaatiosta vastaavan yhtiö vastaa valvomokoneiden ohjelmisto- ja rautatason päivityksistä. Toisena vaihtoehtona ICT-Kymi päivittää valvomokoneet ja tämän jälkeen antaa automaatioasennuksista vastaavalle yritykselle käyttöoikeuden muutosten tekemiseen eli tarvittavien valvomo-ohjelmien asennukseen. Kolmas vaih-

toehto on jättää koko TeamViewer-ohjelmiston asennus tekemättä kasvaneiden kustannusten ja työmäärän takia.

Ensimmäisessä vaihtoehdossa automaatioyritys siis päivittäisi valvomokoneet vähintään Windows 7 -käyttöjärjestelmään sekä asentaisi tarvittavat tietoturvaohjelmat ja etähallintaohjelmiston. Tämän lisäksi koneelle asennettaisiin toinen verkkokortti, jolle ICT-Kymi tarjoaisi tarvittavat yhteysmääritykset internetyhteyden luomiseksi. Näin valvomokoneen automaatiopuolen osoitteen määrittäminen ei tarvitsisi puuttua ja internetyhteys olisi mahdollinen Ekamin omien järjestelmien kautta. Vaihtoehtoisesti jokaiselle valvomokoneelle olisi mahdollista hankkia yksilöllinen ja kuukausimaksullinen USB-liitintä käyttävä mobiililiittymä. Mobiililiittyntävaihtoehtoa tarkastellessa on syytä kuitenkin huomioida signaalin kuuluvuus, koska kaikki valvomot ovat joko maan alla taikka rakennusten alimmassa kerroksessa.

Tässä vaihtoehdossa valvomokoneiden ylläpito jäisi todennäköisesti automaatioyrittäjän vastuulle.

Toisessa vaihtoehdossa ICT-Kymi hankkisi uudet valvomokoneet ja asentaisi niiden laitteiston ja ohjelmiston vastaamaan ICT-Kymin tämän hetkistä vaatimustasoa. Tällöin ICT-Kymi vastaisi myös TeamViewer-ohjelmiston asentamisesta. Rakennusautomaatiota vastaavilta osin automaatioyritys saisi valvomokoneisiin käyttöoikeudet tarvittavien automaatio-sovellusten asentamista ja ylläpitoa varten. Yhteyden luonti tapahtuisi ensimmäisen vaihtoehdon mukaan. Tässä tapauksessa ICT-Kymi todennäköisesti vastaisi valvomokoneiden ylläpidosta automaatio-ohjelmistoja lukuun ottamatta.

Taulukossa 2 on AdConSys Oy:n arvio TeamViewer-ohjelmiston asennuskustannuksista alkuperäisen suunnitelman mukaan, jossa ainoana työnä olisi kyseisen etähallinta-ohjelmiston lisäksi Ekamin valvomokoneiden verkkoyhteyden salliminen.

## **TAULUKKO 2. Kustannusarvio TeamViewer-ohjelmiston asennuksesta**

Hankinta	Kustannusarvio, alv 0%
Teamviewer-ohjelmiston asennus	3 000 €

Taulukosta 3 on puolestaan esitetty Teamviewer-ohjelmiston asennusten lisäksi Malmingin ja Haminan kampusten valvomokoneiden Windows XP päivitykset Windows 7 –käyttöjärjestelmään sekä valvomokoneille lisättävät verkkokortit. Tarjous ei koske Ekamin Comsystem 2000- ja Haminan T.A.C -valvomokoneita, joiden päivittäminen ei laitteiston ja ohjelmistojen iän takia ole mahdollista.

**TAULUKKO 3. Kustannusarvio TeamViewer-ohjelmiston ja uuden Windowsin asennuksesta**

Hankinta	Kustannusarvio, alv 0%
Teamviewer-ohjelmiston asennus, käyttöjärjestelmän ja laitteiston päivitys	8 200 €

Molemmissa tapauksissa tilaajan tulee hankkia omaa käyttötarkoitusta vastaava TeamViewer 11 -lisenssi. Vaihtoehtoina on neljä kokoluokkaa, joita ovat siis Business, Premium, Corporate ja Enterprise. Näistä Ekamille sopivin olisi Premium-versio, joka mahdollistaa rajoittamattoman määrän asennuksia, 400 ohjattavaa laitetta ja yhden samanaikaisen käyttäjän. Näistä samanaikaisien käyttäjien määrä on tarpeen mukaan laajennettavissa. Kyseisen lisenssin hinta kirjoitushetkellä oli 1 149 €.

**6.2 Citect Web-server ja ARENA AX**

Kuten TeamViewer-vaihtoehdossa myös keskitetyssä ratkaisussa kaikki Ekamin sisäverkon ulkopuolelle yhteydessä olevat laitteet tulee päivittää vähintään Windows 7 -käyttöjärjestelmään. Tämän lisäksi järjestelmille tulisi luoda yksi yhteinen sisäverkko, joka kautta kampusten automaatiojärjestelmät voivat olla yhteydessä toisiinsa. Seuraavat kustannusarviot on laatinut AdConsys Oy.

**TAULUKKO 4. Kustannusarvio keskitetystä LVI-automaatioratkaisusta**

Hankinta	Kustannusarvio, alv 0%
Citect Web-server-lisenssi ja työt	17 200 €
ARENA AX ohjelmistopaketti ja työt	19 400 €

Taulukossa 4 on esitetty Citect- ja ARENA AX -ohjelmistoon perustuvan keskitetyn automaatiopalvelimen hinta-arvio. Molemmissa ratkaisuissa jokin valvomokoneista muutettaisiin kampusten yhteiseksi palvelimeksi. Tilaajan tulisi hankkia tälle palveli-

melle kiinteä IP-osoite yhteyden luontia varten. Toinen vaihtoehto olisi liittää automaatioverkkoon Tosibox Lock -laite. Tällöin yhteyden muodostamiseen palvelimelle tarvittaisiin oma fyysinen USB-avain jokaista käyttäjää kohden. Tämän puolestaan nostaisi järjestelmäpäivityksen kustannuksia. Taulukossa 5 näkyy erillishintoja Tosibox-laitteille sekä kolmen vuoden F-secure lisenssille.

#### **TAULUKKO 5. Mahdollisten lisähankintojen erillishintoja**

Hankinta	Erillishinta/kpl, alv 0%
Tosibox Lock	405 €
Tosibox USB-key	180 €
F-secure tietoturvaohjelmisto (3 vuotta)	100 €

Järjestelmien monimutkaisuudesta johtuen arvio toteutuksen työmäärästä on vain suuntaa antava. Tarkempi suunnittelu tulee toteuttaa yhteistyössä automaatiourakoitsijan kanssa. Kumpikaan keskitetyn automaatiopalvelimen vaihtoehtoista ei sisällä Haminan kampuksen T.A.C-valvomoon kytkettyä vanhaa automaatiojärjestelmää.

## **7 POHDINTA**

Tämän työn tavoitteena oli selvittää eri tapoja toteuttaa LVI-automaation etähallinta sekä kuinka niitä voitaisiin hyödyntää Etelä-Kymenlaakson ammattiopistojen kampuksilla. Tämän lisäksi vaihtoehtojen tulisi olla hyödyllisiä LVI-laitteiston ja siihen liittyvän automaation kanssa työskenteleville henkilöstölle sekä Ekamin yhteistyökumppaneille.

Rajauksista huolimatta työn laajuus eri laitteistoista sekä ohjelmistoista johtuen oli jo alusta alkaen huomattava suuri. Tästä johtuen opinnäytetyössä pyrittiin pitäytymään pääosin yleisellä tasolla huomioimalla kuitenkin Ekamin kampusten automaatiojärjestelmien erityispiirteet. Opinnäytetyötä varten tehtiin kattava kirjallisuuskatsaus kohderakennusten automaatiojärjestelmien protokollista sekä yleisistä tietoliikennestandardeista. Työtä varten haastateltiin kampusten automaatiojärjestelmäratkaisusta vastaavia alan asiantuntijoita, joiden kanssa selvitettiin useita vaihtoehtoja toteuttaa toimiva ratkaisu internetin yli tapahtuvaan LVI-automaation hallintaan. Tämän lisäksi suoritettiin myös Ekamin LVI-automaatiolaitteiden kartoitus. Tämän perusteella voitiin luoda hyödyllinen topologiakartta, josta on nopeasti nähtävissä nykyisten järjestelmien kes-

keisimmät osat. Työlle asetetut tavoitteet saavutettiin ja kolme toteutuskelpoista etähallinta vaihtoehtoa valittiin lähempää tarkastelua varten.

Insinööriyön edetessä kävi selväksi, että mahdollisia etähallintaan tarkoitettuja tuotteita on markkinoilla runsaasti. Monet näistä mahdollistivat usean eri järjestelmän yhdistämisen toisiinsa, jolloin toisistaan eroavia toteutusvaihtoehtoja oli monia. Työhön pyrittiin saamaan käytettävissä olevien resurssien puitteissa mahdollisimman monipuolinen otanta laite- ja ohjelmisto pohjaisista ratkaisuista yhden sekä useamman laiteen ohjaamiseen.

Lähempää tarkastelua varten valittiin ohjelmistopohjainen vaihtoehto, joka tarjosi vielä kohonneiden kustannustenkin jälkeen edullisen ja helpon etähallintaratkaisun. Ohjelmalla kampusten henkilökunta saisi käyttökokemuksia etähallinnan mahdollisuuksista. Tämän lisäksi se tarjoaisi mahdollisuuden Ekamin valituille yhteistyökumppaneille pääsyn osaan nykyisiin järjestelmiin.

Kattavampaa hallintaa varten täytyy nykyistä LVI-automaatiojärjestelmää päivittää sekä ohjelmisto että laitteisto puolelta. Näistä ensimmäisenä vaihtoehtona olisi päivittää jokin nykyisistä valvomo-ohjelmistoista tukemaan etäyhteyksiä ja suurempaa laitekantaa. Toinen vaihtoehto olisi investoida uuteen valvomo-ohjelmistoon, joka tukisi suoraan Ekamin uusimpia LVI-automaatiolaitteita. Jälkimmäisen vaihtoehdon etuina vanhaan järjestelmään verrattuna olisi suora laitteistotoimittajan tekninen tuki sekä helpommat laajennusmahdollisuudet muihin automaatiostandardeihin kuten valaistuksen ohjaukseen.

Nykyaikaiset automaatiojärjestelmät ovat monenlaista osaamista vaativia kokonaisuuksia. Näin ollen toimivan ratkaisun toteuttaminen vaatii useamman tahon yhteistyötä. Tässä työssä käsiteltiin lähinnä hallinto- ja alakeskustason ratkaisuja. Järjestelmien päivittäminen vaatii kuitenkin kaikkien tasojen huomioimisen täydellisen yhteensopivuuden ja toimivuuden takaamiseksi. Lisäksi tässä työssä käsiteltiin tietoturvaa lähinnä Ekamin Windows-pohjaisien laitteiden näkökulmasta. Ennen päivittämistä tulisikin uusien ohjelmistojen ja laitteiden vaikutuksista tehdä kattava riskianalyysi.



Ekamin tapauksessa etenkin tulevaisuuden pitkäaikaisempaa järjestelmää suunniteltaessa olisi eri alojen asiantuntijoiden hyvä pitää määrittelytapaaminen, jossa käytäisiin läpi rakennusautomaation tulevaisuuden näkymät, mitä rakennusautomaatio mahdollistaa nykyään, mitä tilaaja ja loppukäyttäjä tarvitsevat sekä miten toteutettava järjestelmä saadaan toimimaan nykyisten IT-järjestelmien kanssa. Näin saataisiin hyvä pohja tulevaisuuden rakennusautomaatioinvestoinneille.

## **8 YHTEENVETO**

Ekamin kampusten automaatiojärjestelmät edustavat kirjavaa kokoelmaa eri aikakausien automaatoratkaisuista. Osaa vanhimmista järjestelmistä on viimevuosien aikana ehditty jo uusimaan ja tarve tämän työn jatkamiselle vielä käytössä olevien järjestelmien kohdalla kasvaa vuosittain.

Vaikka juuri nyt ei akuuttia tarvetta täysmittaiselle LVI-automaation etähallinnalle nähtäisi, on tärkeä huomioida, että nykyisillä päätöksillä on kauaskantoiset seuraukset tulevaisuuden automaatoratkaisuja ajatellen, joten päätös mihin suuntaan Ekamin LVI-automaatiota lähdetään kehittämään laitteistoja uusittaessa tulisi tehdä mahdollisimman pian.

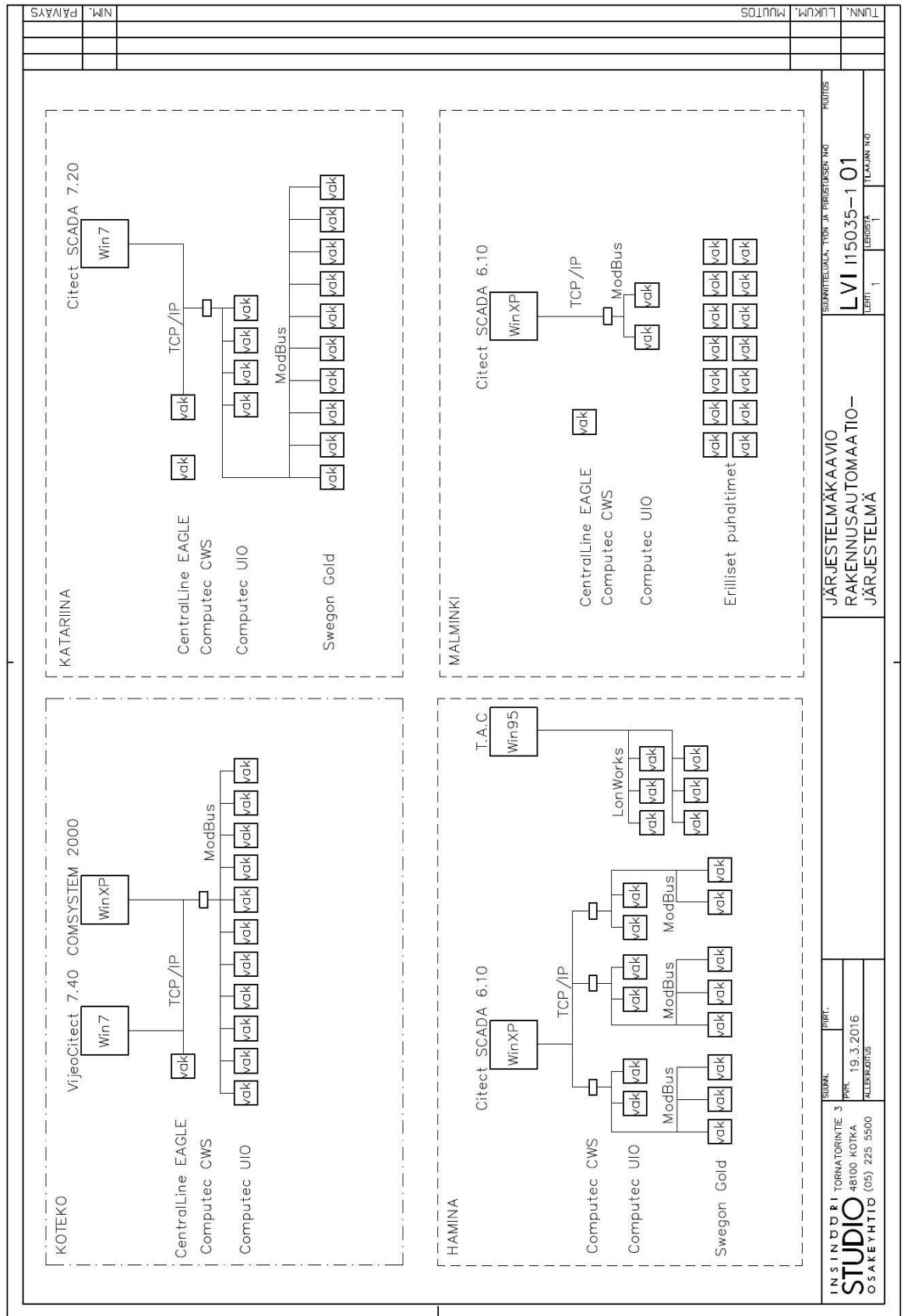
## LÄHTEET

- /1./ Piikkilä, Veijo 2006. Kiinteistöjen tiedonsiirtoväylät ST-käsikirja. Espoo: Sähköinfo Oy
- /2./ Holttinen, Jarmo ja Cisco Press 2002. Ciscon verkkoakatemia: 1. vuosi. Helsinki: Edita
- /3./ Acromag 2005. Introduction to Modbus TCP/IP. WWW-dokumentti. [https://scadahacker.com/library/Documents/ICS\\_Protocols/Acromag%20-%20Introduction%20to%20Modbus-TCP.pdf](https://scadahacker.com/library/Documents/ICS_Protocols/Acromag%20-%20Introduction%20to%20Modbus-TCP.pdf). Ei päivitystietoa. Luettu 21.3.2016.
- /4./ Modbus Organization 2006. MODBUS over Serial Line Specification and Implementation Guide V1.02. WWW-dokumentti. [http://www.modbus.org/docs/Modbus\\_over\\_serial\\_line\\_V1\\_02.pdf](http://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf). Päivitetty 20.12.2006. Luettu 18.3.2016.
- /5./ Savinen, Marika 2016. Haastattelu 9.3.2016. Adconsys Oy
- /6./ Modbus Organization 2006. MODBUS MESSAGING ON TCP/IP IMPLEMENTATION GUIDE V1.0b. WWW-dokumentti. [http://www.modbus.org/docs/Modbus\\_Messaging\\_Implementation\\_Guide\\_V1\\_0b.pdf](http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf). Päivitetty 24.10.2006. Luettu 21.3.2016.
- /7./ Modbus organization 2012. Modbus application protocol specification V1.1b3. WWW-dokumentti. [http://www.modbus.org/docs/Modbus\\_Application\\_Protocol\\_V1\\_1b3.pdf](http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf). Päivitetty 26.4.2012. Luettu 19.3.2016.
- /8./ Kaananen, Juha 2010. Opinnäytetyö. PDF-dokumentti. BACnet-protokollan käyttö rakennusautomaatiossa. <http://www.theseus.fi/handle/10024/14435>
- /9./ Thomas, George 2008. WWW-dokumentti. <http://www.bacnetinternational.org/files/Introduction%20to%20BACnet%20Routers.pdf>. Ei päivitystietoa. Luettu 2.4.2016.
- /10./ Bacnet 2016. BACnet/IP. WWW-dokumentti. <http://www.bacnet.org/Tutorial/BACnetIP/index.html>. Ei päivitystietoa. Luettu 2.4.2016.
- /11./ Savinen, Marika 2016. Haastattelu 4.3.2016. Adconsys Oy
- /12./ Savinen, Marika 2016. Sähköposti 1.3.2016. Adconsys Oy
- /13./ Tani, Iina 2016. Haastattelu 13.4.2016. ICT-Kymi
- /14./ Tani, Iina 2016. Haastattelu 22.4.2016. ICT-Kymi

- /15./ Microsoft 2016. WWW-dokumentti. <https://support.microsoft.com/fi-fi/lifecycle?C2=9980>. Päivitetty 12.1.2016. Luettu 15.4.2016.
- /16./ Microsoft 2016. WWW-dokumentti. <http://windows.microsoft.com/en-us/windows/lifecycle>. Päivitetty tammikuu 2016. Luettu 15.4.2016.
- /17./ TeamViewer GmbH 2016. WWW-dokumentti. <http://download2.teamviewer.com/docs/fi/TeamViewer-Security-Statement-fi.pdf>. Päivitetty 1.2016. Luettu 15.2.2016.
- /18./ Intel 2016. Remote Wake up Basics for Intel® Ethernet Products. WWW-dokumentti. <http://www.intel.com/content/www/us/en/support/network-and-i-o/ethernet-products/000005793.html>. Päivitetty 3.3.2016. Luettu 7.3.2016
- /19./ Lantronix 2013. WWW-dokumentti. [http://www.lantronix.com/wp-content/uploads/pdf/Spiders\\_UG.pdf](http://www.lantronix.com/wp-content/uploads/pdf/Spiders_UG.pdf). Päivitetty marraskuu 2013. Luettu 20.3.2016.
- /20./ Tosibox 2015. Lock 200 & Key 200 User Manual v1.2. WWW-dokumentti. [http://www.tosibox.com/wp-content/library/technical/User%20Manual/Lock%20User%20Manual/Tosibox\\_User\\_Manual\\_en.pdf](http://www.tosibox.com/wp-content/library/technical/User%20Manual/Lock%20User%20Manual/Tosibox_User_Manual_en.pdf). Päivitetty 1.5.2015. Luettu 15.3.2016.
- /21./ Laine, Harri 2016. Haastattelu 11.3.2016. Fidelix Oy
- /22./ Support 2016. Haastattelu 17.3.2016. Tosibox
- /23./ Ylimartimo, Veikko 2016. Haastattelu 14.3.2016. Tosibox
- /24./ Lantronix 2006. UDS1100 User Guide. WWW-dokumentti. [http://www.lantronix.com/wp-content/uploads/pdf/UDS1100-IAP\\_UG.pdf](http://www.lantronix.com/wp-content/uploads/pdf/UDS1100-IAP_UG.pdf). Päivitetty 6.6.2006. Luettu 12.2.2016.
- /25./ Lantronix 2005. Modbus Protocol User Guide. WWW-dokumentti. [http://www.lantronix.com/wp-content/uploads/pdf/UDS1100-IAP\\_Modbus-UG.pdf](http://www.lantronix.com/wp-content/uploads/pdf/UDS1100-IAP_Modbus-UG.pdf). Päivitetty 9.10.2005. Luettu 13.2.2016.
- /26./ Latvasalo, Marko 2016. Haastattelu 16.3.2016 Schneider Electric
- /27./ Schneider Electric. WWW-dokumentti. [http://www2.schneider-electric.com/resources/sites/SCHNEIDER\\_ELECTRIC/content/live/FAQS/233000/FA233540/en\\_US/SCADA%20Catalog.pdf](http://www2.schneider-electric.com/resources/sites/SCHNEIDER_ELECTRIC/content/live/FAQS/233000/FA233540/en_US/SCADA%20Catalog.pdf). Ei päivitystietoa. Luettu 1.4.2016.
- /28./ Schneider Electric. WWW-dokumentti. [http://www2.schneider-electric.com/resources/sites/SCHNEIDER\\_ELECTRIC/content/live/FAQS/275000/FA275530/en\\_US/Vijeo-Compatibility-Matrix-A5-Jun2015.pdf](http://www2.schneider-electric.com/resources/sites/SCHNEIDER_ELECTRIC/content/live/FAQS/275000/FA275530/en_US/Vijeo-Compatibility-Matrix-A5-Jun2015.pdf). Päivitetty kesäkuu 2015. Luettu 2.5.2016.

- /29./ Pim, Ivan 2016. Sähköposti 26.2.2016. Lantronix
- /30./ Central Line 2014. ARENA AX - BACnet Supervisor Product Data. WWW-dokumentti. <http://products.centraline.com/en/pdf/en0z0945-ge51r0314.pdf>. Ei päivitystietoa. Luettu 2.3.2016.
- /31./ Väkevä, Jarmo 2016. Sähköposti 2.5.2016. Adconsys Oy

## Ekamin LVI-automaation nykyinen topologia



Ekamin LVI-automaation topologiasta ehdotus

